

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.: 23-CV-60830-RAR (and all consolidated actions)

ARIANA SKURAUSKIS, *et al.*, *on behalf of
themselves and all others similarly situated,*

Plaintiffs,

v.

NATIONSBENEFITS HOLDINGS, LLC, *et al.*,

Defendants.

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Lenore Caliendo, Kimberly Dekenipp, T.E., Renee Fideleff, Leroy Fuss, Teresa Hassan, Jeffery King, Barbara Kosbab, Lawrence Kosbab, Mary Ann Landries, Pamela Lazaroff, Steven Lazaroff, Kevin McCoy, Sharon McCoy, Catherine Radke, Martin Radke, Dezarae Sanders, Arnisha Marie Shepherd, Ariana Skurauskis, Anthony Skuya, A.T., Michael Wanser, Edward Wilczynski, Sara Jean Williams, Wanda Wilson, and Stephen Wolsey (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint action against NationsBenefits, LLC and NationsBenefits Holdings, LLC (collectively, “NationsBenefits”). The following allegations are based upon Plaintiffs’ personal knowledge as to their own actions and their counsels’ investigations, facts of public record, and upon information and belief as to all other matters.

1. This action arises from NationsBenefits’ failure to secure the sensitive Private Information (defined herein) of Plaintiffs and the proposed Class and Subclasses (defined herein) for whom NationsBenefits performed services.

2. NationsBenefits is a health benefits administration company that partners with managed care organizations to provide supplemental benefits, flex cards, and member engagement

solutions. In this role, for years, NationsBenefits directly and indirectly collected highly sensitive personal identifiable information (“PII”) and protected health information (“PHI”) (PII and PHI collectively “Private Information”) from millions of its own clients and the customers of its partner health insurance organizations. Despite having duties created by statute and common law to safeguard that Private Information entrusted to it, NationsBenefits allowed information concerning millions of people to be stolen and then sold on the dark web by a notorious cybercriminal organization.

3. On April 13, 2023, NationsBenefits disclosed that months earlier over 3,000,000 individuals’ Private Information in its care had been stolen in a massive data breach (“Data Breach”). A cybercriminal group called the “Clop ransomware gang” (“Clop”), known for its attacks against the healthcare sector, took credit for exfiltrating vast amounts of unencrypted, highly sensitive information from NationsBenefits’ file transfer program. Indeed, other cybercriminal groups may also have taken advantage of this vulnerability, increasing the severity of the Data Breach.

4. NationsBenefits admits these cybercriminals stole Plaintiffs’ Private Information as part of the Data Breach. However, on information and belief, Clop gave NationsBenefits the opportunity to repurchase all the stolen data, but NationsBenefits refused to pay the ransom. As a result, Clop is believed to have sold that Private Information on the dark web.

5. As a result of NationsBenefits’ impermissibly lax data security practices, Plaintiffs and Class Members are at a present and continuing risk for identity and medical identity theft. NationsBenefits then compounded this harm by waiting more than two months before notifying affected consumers that their highly sensitive Private Information was now in the hands of sophisticated cyber criminals.

6. Fortra LLC (“Fortra”), which provides information technology management software and services to NationsBenefits, learned about the Data Breach on or about January 30, 2023. That same week, on February 3, 2023, Fortra informed NationsBenefits about the Data Breach and

provided suggestions for mitigation measures. Nevertheless, NationsBenefits inexplicably waited until February 7, 2023, to implement the suggested mitigation measures.

7. It was not until April 13, 2023, over two months later, that NationsBenefits first began notifying Class Members of the Data Breach. Even worse, they did not inform all affected consumers at once. Many Class Members, including Plaintiffs, did not even learn until weeks later that cybercriminals had stolen their information. NationsBenefits' inexcusable delays permitted the cybercriminals' greater access to its servers and prevented Class Members from taking immediate defensive measures to protect their valuable Private Information. *See* Ex. A (Exemplar Notice Letter).

8. The Data Breach was a direct result of NationsBenefits' deficient cybersecurity practices, and the wealth of information and warnings available to NationsBenefits makes its failures even more egregious.

9. Taking reasonable, standard precautions against cybercrime and data breaches is a fundamental duty of doing business in the modern age—especially for businesses that profit from analyzing and processing Private Information. By collecting, maintaining, and profiting from Plaintiffs' and Class Members' Private Information, NationsBenefits was required by law to exercise reasonable care and comply with industry and statutory requirements to protect that information—and it failed to do so.

10. Among myriad industry standards and statutes for protection of sensitive information, health care information is specifically governed by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. HIPAA requires entities like NationsBenefits to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI, establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

11. Instead, NationsBenefits' woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence. NationsBenefits disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement reasonable measures to safeguard its customers' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information.

12. The highly sensitive information exfiltrated in the Data Breach includes, but is not limited to, full names, dates of birth, Social Security numbers, phone numbers, addresses, gender, health plan subscriber information, including identification numbers, and Medicare numbers.

13. By aggregating information obtained from the Data Breach with other sources, or other methods, criminals can assemble a full dossier of Private Information on an individual in order to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names, birth dates, Social Security numbers, and addresses to open new financial accounts, incur charges in credit, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it.¹ Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

14. Likewise, the exfiltration of PHI puts Plaintiffs and Class Members at a present and continuing risk for medical identity theft, especially in light of the high demand and value of Medicare

¹ See, e.g., *Report to Congressional Requesters*, U.S. GOV'T ACCOUNTABILITY OFFICE (June 2007), <http://www.gao.gov/assets/270/262899.pdf>; Melanie Lockert, *How do hackers use your information for identity theft?*, CREDITKARMA (Oct. 1, 2021), <https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information>; Ravi Sen, *Here's how much your Private Information is worth to cybercriminals—and what they do with it*, PBS (May 14, 2020), <https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it>; Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LIFELOCK BY NORTON (Feb. 4, 2021), <https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft>.

identification numbers on the dark web.² Medical identity theft poses an even more critical threat to victims—medical fraud could lead to loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring substantial medical debt.

15. Due to the highly valuable nature of PHI, the FBI has warned healthcare providers that they are likely to be the targets of cyberattacks like the attack that caused the Data Breach.³

16. Adding insult to injury, there has been no assurance offered by NationsBenefits that all personal data or copies of data have been recovered or destroyed, or that NationsBenefits has adequately enhanced its security practices or dedicated sufficient resources and staff and to avoid a similar breach of its network in the future.

17. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to, present and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; ongoing monetary loss and economic harm, including loss of value of their Private Information; loss of value of privacy and confidentiality of the stolen Private Information; illegal sales of the compromised Private Information; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries.

18. Plaintiffs and Class Members would not have provided their valuable PII and sensitive PHI to their respective health plans or other entities to in turn provide that information to NationsBenefits had they known that NationsBenefits would make the Private Information internet-accessible, not encrypt personal and sensitive data elements such as Social Security numbers, Medicare

² *What to Know About Medical Identity Theft*, FED. TRADE COMM'N (May 2021), <https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft>.

³ Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS (Aug. 20, 2014), <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820>.

numbers, health insurance identification numbers, and dates of birth, and not delete the Private Information it no longer had reason to maintain.

19. Through this lawsuit, Plaintiffs seek to hold NationsBenefits responsible for the injuries it inflicted on Plaintiff and approximately 3,000,000 similarly situated people due to its impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information which remains in the possession of NationsBenefits.

I. JURISDICTION AND VENUE

20. This Court has original subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d)(2), because the amount in controversy for the Class and State Subclasses exceeds the sum of \$5,000,000, exclusive of interest and costs, there are more than 100 Class Members, and minimal diversity exists because many Class Members are citizens of a different state than NationsBenefits.

21. This Court has personal jurisdiction over NationsBenefits. Upon information and belief, NationsBenefits LLC’s sole member, Glenn Parker, resides in Fort Lauderdale, Florida, and is a citizen of the state of Florida. On information and belief, Glenn Parker is also the sole member of NationsBenefits Holdings LLC. NationsBenefits’ headquarters and principal place of business is in Plantation, Florida.

22. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), (b)(2), and (c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and NationsBenefits conducts substantial business in this District. In addition, on information and belief, Plaintiffs’ and Class Members’ Private Information was maintained within this District.

II. PARTIES

A. Plaintiffs

Lenore Caliendo

23. Plaintiff Lenore Caliendo is a resident and citizen of Illinois.

24. Plaintiff Caliendo receives benefits from NationsBenefits by virtue of her health plan membership with Aetna Medicare Advantage.

25. Plaintiff Caliendo received a letter from NationsBenefits concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Caliendo's name, address, telephone number, date of birth, gender, health plan subscriber ID number, Social Security number, and/or Medicare number. Plaintiff Caliendo has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

26. Plaintiff Caliendo was the victim of medical identity theft following the Data Breach. In March 2023, Plaintiff Caliendo was contacted by her health insurance company regarding five suspicious charges for Covid tests between January and April 2023. Those charges were fraudulent, as Plaintiff Caliendo never authorized or received those tests, nor had she ever visited the doctor who ordered those tests. Dealing with the consequences of the Data Breach has become a daily occurrence for Plaintiff Caliendo, who receives approximately 4 to 5 spam calls each day, along with spam emails and text messages. Plaintiff Caliendo has spent approximately 20 hours addressing the Data Breach, including spending approximately 2 hours on the telephone with NationsBenefits trying to get more information about the Data Breach, opening a new bank account and closing her old account, changing her billing information, visiting a Social Security office to change her Social Security check deposit information, and monitoring her accounts and credit report. As a result of the Data Breach, Plaintiff Caliendo experiences anxiety and a feeling of helplessness when checking her accounts or her

insurance, and she remains fearful she will be the victim of identity theft again. Plaintiff Caliendo spends time each week exercising to deal with the stress caused by the Data Breach.

Kimberly Dekenipp

27. Plaintiff Kimberly Dekenipp is a resident and citizen of Texas.

28. Plaintiff Dekenipp receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

29. Plaintiff Dekenipp received a letter dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Dekenipp's name, gender, address, date of birth, health plan subscriber ID number, and Medicare number. Plaintiff Dekenipp has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

30. Plaintiff Dekenipp is anxious that her Private Information is now in unknown hands and fears the risk of identity theft she now faces, including fraud affecting her credit. As a result of the Data Breach, Plaintiff Dekenipp has spent at least 2 hours monitoring her accounts and researching details of the Data Breach. She has also experienced an increase in the amount of intrusive spam calls, texts, and emails she receives. Due to her concern about the Data Breach and identity theft, Plaintiff Dekenipp limited her use of credit following the Data Breach.

T.E.

31. Plaintiff T.E. is a resident and citizen of North Carolina.

32. Plaintiff T.E. receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

33. Plaintiff T.E. received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff T.E.'s name,

address, telephone number, date of birth, gender, health plan subscriber ID number, and Medicare number. Plaintiff T.E. has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

34. Plaintiff T.E. was the victim of identity theft following the Data Breach. Plaintiff T.E. is disabled and receives disability benefits. After the Data Breach occurred, unauthorized charges appeared on Plaintiff T.E.'s Cash App account and her Direct Express federal benefits card. Plaintiff has received numerous calls asking her to activate her NationsBenefits card, though she already possesses a card that has been activated. Plaintiff T.E. has spent approximately 10 hours attempting to mitigate harm from the Data Breach, including monitoring her accounts and credit report and researching ways to protect herself. Plaintiff T.E. has experienced anxiety and frustration as a result of the Data Breach, which required her to obtain an increased prescription for anti-anxiety medication.

Renee Fideleff

35. Plaintiff Renee Fideleff is a resident and citizen of Florida.

36. Plaintiff Fideleff receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

37. Plaintiff Fideleff received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Fideleff's name, address, telephone number, date of birth, gender, health plan subscriber ID number, and Medicare number. Plaintiff Fideleff has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

38. After the Data Breach, Plaintiff Fideleff received an email supposedly from Geek Squad informing her that she was being billed for a transaction she did not authorize, and that she should let them take control of her computer to resolve the issue and attempting to elicit a fee to

cancel the transaction; they harassed Plaintiff Fideleff by phone several times to try to get her to pay the fee. Plaintiff Fideleff also received a letter in the mail regarding a supposed property sale that she was unaware of and did not authorize. She has also experienced an increased number of spam calls, texts, and emails since the Data Breach. Plaintiff Fideleff has spent approximately 1 hour per week monitoring her accounts for fraudulent charges since the Data Breach. As a result of the Data Breach, she is anxious and fearful that she will be the victim of other fraud in the future.

Leroy Fuss

39. Plaintiff Leroy Fuss is a resident and citizen of Pennsylvania.

40. Plaintiff Fuss receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

41. Plaintiff Fuss received a letter dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Fuss' name, address, telephone number, date of birth, gender, and health plan subscriber ID number. Plaintiff Fuss has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

42. Plaintiff Fuss was the victim of identity theft following the Data Breach. Following the Data Breach, several banks, financial institutions, and TransUnion contacted Plaintiff Fuss regarding accounts created in his name that he did not open or authorize. Two accounts Plaintiff Fuss did not open appeared on his credit report. Fraudulent charges also appeared on Plaintiff Fuss' debit card, forcing him to replace that card. These fraudulent charges cost Plaintiff Fuss approximately \$4,800. As a result of the Data Breach and resulting fraudulent charges and accounts, Plaintiff Fuss froze his credit at Experian, Equifax, and TransUnion. Since the Data Breach, he has spent several hours reviewing his accounts, researching news about the Data Breach, attempting to contact NationsBenefits, obtaining his credit reports, freezing his credit, and contact the Social Security

Administration about his Social Security deposits. He has also experienced an increased number of spam calls, texts, and emails since the Data Breach. The extensive fraud Plaintiff Fuss has faced as a result of the Data Breach has caused him anxiety, for which he takes multiple anti-anxiety medications.

Teresa Hassan

43. Plaintiff Teresa Hassan is a resident and citizen of Michigan.

44. Plaintiff Hassan receives benefits from NationsBenefits by virtue of her health plan membership with UAW Retiree Medical Benefits Trust.

45. Plaintiff Hassan received a letter from NationsBenefits dated April 28, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Hassan's name, address, date of birth, gender, health plan subscriber ID number, Social Security number, and Medicare number. Plaintiff Hassan has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

46. Plaintiff Hassan has spent approximately 30 hours attempting to mitigate the effects of the Data Breach, including obtaining her credit report from Experian, Equifax, and TransUnion, reviewing her accounts, and notifying the Social Security Administration that her information was compromised, driving to and visiting her bank, filing a police report, and attempting to call NationsBenefits about the Data Breach. Plaintiff Hassan has experienced an increased number of spam calls since the Data Breach. As a result of the Data Breach, Plaintiff Hassan is anxious and fearful that she will be the victim of identity theft or other fraud.

Jeffery King

47. Plaintiff Jeffery King is a resident and citizen of Ohio.

48. Plaintiff King receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

49. Plaintiff King received a letter from NationsBenefits concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff King's name, gender, address, phone number, date of birth, health plan subscriber ID number, and Medicare number, and other items relating to Plaintiff's receipt of benefits from NationsBenefits. Plaintiff King has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

50. Plaintiff King has been the victim of identity theft following Data Breach. Since the Data Breach, he has received several alerts about unauthorized account inquiries and transactions attempted in his name. Additionally, between approximately late April and early August 2023, several unauthorized transactions appeared on Plaintiff King's Cash App and PayPal accounts. Plaintiff King has experienced an increase in the number of spam calls, texts, and emails he receives since the Data Breach occurred. Plaintiff King has spent approximately 2 hours per week attempting to mitigate the effects of the Data Breach, including obtaining his credit report, monitoring his accounts, checking his credit history, and locking and changing his debit cards. He has limited the use of his credit cards due to the Data Breach. Plaintiff King is highly concerned that his information was exposed in the Data Breach and is fearful he will continue to be the victim of additional fraud in the future.

Barbara Kosbab

51. Plaintiff Barbara Kosbab is a resident and citizen of Ohio.

52. Plaintiff Barbara Kosbab receives benefits from NationsBenefits by virtue of her health plan memberships with Medicare and Anthem Blue Cross Blue Shield ("Anthem").

53. Plaintiff Barbara Kosbab received a letter from NationsBenefits dated April 28, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Barbara Kosbab's name, address, telephone number, date of birth, gender, health plan subscriber ID number,

Social Security number, and Medicare number. Plaintiff Barbara Kosbab has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

54. Plaintiff Barbara Kosbab was the victim of identity theft following the Data Breach. After the Data Breach occurred, Plaintiff Kosbab's Medicare account was charged twelve times for COVID-19 test kits and catheters that she did not order or receive. She has spent time reporting these fraud claims to Medicare and the U.S. Attorney General. Additionally, one credit reporting agency indicated that her Private Information was available on the dark web. Plaintiff Barbara Kosbab has spent approximately 50 hours checking her accounts and medical accounts, reporting any compromises, attempting to contact NationsBenefits about the breach, and changing her billing information. Plaintiff Barbara Kosbab is fearful and anxious that she will be the victim of additional identity theft or other fraud in the future.

Lawrence Kosbab

55. Plaintiff Lawrence Kosbab is a resident and citizen of Ohio.

56. Plaintiff Lawrence Kosbab receives benefits from NationsBenefits by virtue of his health plan memberships with Medicare and Anthem.

57. Plaintiff Lawrence Kosbab received a letter from NationsBenefits dated April 28, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Lawrence Kosbab's name, address, telephone number, date of birth, gender, health plan subscriber ID number, Social Security number, and Medicare number. Plaintiff Lawrence Kosbab has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

58. As a result of the Data Breach, Plaintiff Lawrence Kosbab spends approximately 7 hours per week monitoring his accounts against fraudulent charges. Plaintiff Lawrence Kosbab is

anxious and fearful that he will be the victim of identity theft or other fraud in the future because his information was exposed in the Data Breach.

Mary Ann Landries

59. Plaintiff Mary Ann Landries is a resident and citizen of New York.

60. Plaintiff Landries receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

61. Plaintiff Landries received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Landries' name, address, telephone number, date of birth, gender, and health plan subscriber ID number. Plaintiff Landries has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

62. Plaintiff Landries has experienced a large increase in the number of spam calls and texts she receives since the Data Breach occurred. She has received texts claiming to be from Verizon, but she does not have a Verizon account; additionally, she received a fraudulent text claiming to be from her primary care provider that attempted to elicit her medical information. Plaintiff Landries has spent approximately 15 hours attempting to mitigate the Data Breach, including blocking spam calls and texts and addressing the fraudulent message from her primary care provider. She is fearful and anxious that she may be the victim of identity theft or other fraud in the future because her Private Information was exposed in the Data Breach.

Pamela Lazaroff

63. Plaintiff Pamela Lazaroff is a resident and citizen of Arkansas.

64. Plaintiff Pamela Lazaroff receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

65. Plaintiff Pamela Lazaroff received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Pamela Lazaroff's name, address, telephone number, date of birth, gender, and health plan subscriber ID number. Plaintiff Pamela Lazaroff has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

66. As a result of the Data Breach, Plaintiff Pamela Lazaroff was the victim of identity theft, as an unknown person attempted to open a credit or debit card account in her name. Since the Data Breach, Plaintiff Pamela Lazaroff has experienced an increased number of phishing attempts and spam text messages. Plaintiff Pamela Lazaroff is anxious about identity theft and has spent approximately 10 hours monitoring her credit and checking her accounts.

Plaintiff Stephen Lazaroff

67. Plaintiff Stephen Lazaroff is a resident and citizen of Arkansas.

68. Plaintiff Stephen Lazaroff receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

69. Plaintiff Stephen Lazaroff received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Stephen Lazaroff's name, gender, address, telephone number, date of birth, health plan subscriber ID number, Social Security number, and Medicare number. Plaintiff Lazaroff has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

70. Since the Data Breach occurred, Plaintiff Stephen Lazaroff has experienced an increased number of spam calls, text messages, and emails. Plaintiff Stephen Lazaroff is anxious and

fearful that he will be the victim of identity theft or other fraud in the future because his information was exposed in the Data Breach.

Kevin McCoy

71. Plaintiff Kevin McCoy is a resident and citizen of Illinois.

72. Plaintiff Kevin McCoy receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

73. Plaintiff Kevin McCoy received a letter from NationsBenefits dated April 28, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Kevin McCoy's name, address, telephone number, date of birth, gender, health plan subscriber ID number, Social Security number, and Medicare number. Plaintiff Kevin McCoy has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

74. As a result of the Data Breach, Plaintiff Kevin McCoy has experienced anxiety and fear of identity theft and has placed a fraud alert on his credit cards.

Plaintiff Sharon McCoy

75. Plaintiff Sharon McCoy is a resident and citizen of Illinois.

76. Plaintiff Sharon McCoy receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

77. Plaintiff Sharon McCoy received a letter from NationsBenefits dated April 28, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Sharon McCoy's name, address, date of birth, gender, health plan subscriber ID number, Social Security number, and Medicare number. Plaintiff Sharon McCoy has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

78. Plaintiff Sharon McCoy has been informed that her confidential information is on the dark web. She spent time visiting her bank and putting a fraud alert on her account. She is fearful and anxious that she may be the victim of identity theft or other fraud in the future because her Private Information was exposed in the Data Breach.

Catherine Radtke

79. Plaintiff Catherin Radtke is a resident and citizen of Michigan.

80. Plaintiff Catherine Radtke receives benefits from NationsBenefits by virtue of her health plan membership with HAP/Medicare through the UAW Retiree Medical Benefits Trust.

81. Plaintiff Catherine Radtke received a letter from NationsBenefits dated April 28, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Catherine Radtke's name, address, date of birth, gender, health plan subscriber ID number, Social Security number address, and Medicare number. Plaintiff Catherine Radtke has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

82. As a result of the Data Breach, Plaintiff Catherine Radtke is fearful and anxious that she may be the victim of identity theft or other fraud in the future because her Private Information was exposed in the Data Breach.

Martin Radtke

83. Plaintiff Martin Radtke is a resident and citizen of Michigan.

84. Plaintiff Martin Radtke receives benefits from NationsBenefits by virtue of his health plan membership with HAP/Medicare.

85. Plaintiff Martin Radtke received a letter from NationsBenefits dated April 28, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Martin Radtke's

name, address, telephone number, date of birth, gender, health plan subscriber ID number, Social Security number, and Medicare number. Plaintiff Martin Radtke has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

86. As a result of the Data Breach, Plaintiff Martin Radtke has experienced an increase in phishing attempts and spam. Indeed, Plaintiff Martin Radtke has spent approximately 24 hours, on behalf of himself and his wife (Plaintiff Catherine Radtke), monitoring their accounts, including checking their credit card accounts daily, and attempting to contact NationsBenefits for information about the Data Breach. Plaintiff Martin Radtke now constantly worries about his financial accounts and using health insurance products, and he remains fearful and anxious that he will be the victim of identity theft or other fraud in the future.

Plaintiff Dezae Sanders

87. Plaintiff Dezae Sanders is a resident and citizen of Texas.

88. Plaintiff Sanders receives benefits from NationsBenefits by virtue of her health plan membership administered by Anthem.

89. Plaintiff Sanders received a letter from NationsBenefits dated April 13, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Sanders' name, address, date of birth, gender, health plan subscriber ID number, and Social Security number. Plaintiff Sanders has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

90. As a result of the Data Breach, Plaintiff Sanders was the victim of identity theft. Fraudulent charges appeared on her credit card, forcing her to close that account. She has also experienced an increase in the number of spam calls, texts, and emails she receives. She has spent approximately 20 hours attempting to mitigate the Data Breach, including attempting to contact NationsBenefits for information, changing billing information, monitoring her accounts, and checking

her credit report every month. Plaintiff Sanders is fearful and anxious that she will be the victim of additional identity theft or fraud in the future.

Arnisha Marie Shepherd

91. Plaintiff Arnisha Shepherd is a resident and citizen of Indiana.

92. Plaintiff Shepherd receives benefits from NationsBenefits by virtue of her health plan membership with Anthem.

93. Plaintiff Shepherd received a letter from NationsBenefits dated April 13, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Shepherd's name, address, telephone number, date of birth, gender, health plan subscriber ID number, and Social Security number. Plaintiff Shepherd has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

94. Since the Data Breach, Plaintiff Shepherd has experienced several hard inquiries on her credit files related to an application for credit at a bank she did not make nor authorize and, further, an AT&T account was opened in her name and without her knowledge or consent. In addition, someone used her bank debit card to make an unauthorized restaurant purchase. Plaintiff Shepherd has had to spend many hours of her time and effort to monitor her credit reports and take steps to close her debit card account on which the unauthorized purchase was made. She spent time and effort resetting her other accounts that were on automatic billing after the issue with the AT&T account, monitoring her credit, and adding security freezes to her credit files. Since the Data Breach, Plaintiff Shepherd has received increased calls and texts that she does not recognize. As a result of the Data Breach, Plaintiff Shepherd is very anxious that her private information is in unknown hands and is being misused, and she is fearful that she will face additional fraud in the future.

Ariana Skurauskis

95. Plaintiff Ariana Skurauskis is a resident and citizen of California.

96. Plaintiff Skurauskis receives benefits from NationsBenefits by virtue of her health plan membership with Santa Clara Family Health Plan.

97. Plaintiff Skurauskis received a letter from Santa Clara Family Health Plan dated April 21, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Skurauskis' name, contact information, date of birth, Santa Clara Family Health Plan ID number, and Medi-Cal Index Number. Plaintiff Skurauskis has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

98. Plaintiff Skurauskis was the victim of identity theft following Data Breach. After the Data Breach, a large unauthorized charge appeared on her PayPal account. Additionally, in February 2023 an unknown person accessed her Forever 21 account and attempted to purchase items worth \$328.88. Plaintiff Skurauskis has also experienced an increased number of phishing calls and spam text messages since the Data Breach. After the Data Breach, Plaintiff Skurauskis placed a freeze on her credit. Plaintiff Skurauskis is fearful that she will continue to experience identity theft in the future, causing her to lose money, take on increased debt, and negatively affecting her credit score. Plaintiff Skurauskis has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

Anthony Skuya

99. Plaintiff Anthony Skuya is a resident and citizen of Florida.

100. Plaintiff Skuya receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

101. Plaintiff Skuya received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Skuya's name, address, telephone number, date of birth, gender, and health plan subscriber ID number. Plaintiff Skuya has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

102. Plaintiff Skuya has spent approximately 2 hours researching the Data Breach and monitoring his accounts for fraudulent activity. He has experienced an increased number of spam calls and texts. Plaintiff Skuya received one call from someone who had his name and address and attempted to elicit his Medicare information. He has experienced increased fear and anxiety because his Private Information is on the dark web and because he faces a continuing risk of identity theft in the future.

A.T.

103. Plaintiff A.T. is a resident and citizen of Kansas.

104. Plaintiff A.T. receives benefits from NationsBenefits by virtue of his health plan membership with Aetna Medicare Advantage.

105. Plaintiff A.T. received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff A.T.'s name, address, telephone number, date of birth, gender, health plan subscriber ID number, and Medicare number. Plaintiff A.T. has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

106. Plaintiff A.T. was the victim of identity theft following the Data Breach. After the Data Breach occurred, multiple attempts were made by an unknown person to access Plaintiff A.T.'s Walmart account to which his debit cards are linked. Plaintiff A.T. had to take the time and effort to

add two-step authentication to his Walmart account. Plaintiff A.T. has spent approximately 25 to 30 hours addressing the attempts to access his Walmart account, changing his Walmart account to use the two-step authentication process, investigating the Data Breach, and monitoring his accounts and credit report. He has also experienced an increase in the number of spam calls, emails, and text messages he receives. Plaintiff A.T. is anxious that his medical information and Medicare information were compromised in the Data Breach, and is afraid they might be further disclosed and misused. The Data Breach has caused Plaintiff A.T. to experience anxiety and fear, for which he now takes anxiety medication and spends approximately 1.5 hours each week meditating to try to remedy.

Michael Wanser

107. Plaintiff Michael Wanser is a resident and citizen of New York.

108. Plaintiff Wanser receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

109. Plaintiff Wanser received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Wanser's name, address, telephone number, date of birth, gender, health plan subscriber ID number, and Medicare number. Plaintiff Wanser has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

110. As a result of the Data Breach, Plaintiff Wanser has experienced an extremely high increase in the number of spam calls and texts he receives. Each day he gets more than 20 spam calls on his cell phone, and more than 5 spam calls on his home phone. He also receives approximately 2 to 3 spam text messages every day. The Data Breach has caused Plaintiff Wanser increased fear and anxiety about the misuse of his Private Information and the potential impact on his credit. Since the Data Breach he has spent approximately 1 to 2 hours each week monitoring his accounts for

fraudulent activity. Plaintiff Wanser is anxious and fearful that he will be the victim of identity theft or other fraud in the future because his information was exposed in the Data Breach.

Edward Wilczynski

111. Plaintiff Edward Wilczynski is a resident and citizen of the State of New Jersey.

112. Plaintiff Wilczynski receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

113. Plaintiff Wilczynski received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Wilczynski's name, address, telephone number, date of birth, gender, health plan subscriber ID number, Medicare number, and other items relating to Plaintiff's receipt of benefits from NationsBenefits. Plaintiff Wilczynski has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

114. Plaintiff Wilczynski was the victim of identity theft following the Data Breach. Between May and July 2023, he twice had to cancel his debit card. Plaintiff Wilczynski's bank notified him that there was a security breach on his account, and that someone was trying to take money out of his account using his debit card number. After the first incident, Plaintiff Wilczynski cancelled the card and the bank re-issued it. Then this incident happened again within a month. Plaintiff closed his account because he was concerned about account security and then opened a new account at another bank. He has also noticed an increase of spam messages. As a result of the breach, Plaintiff Wilczynski has spent 12 to 14 hours monitoring his financial accounts and statements and remedying the fraud he experienced at his bank. He had to drive 40 minutes to his bank twice, burning approximately \$20 worth of fuel. As a result of the breach, he is anxious that individuals will become the victim of future identity fraud or theft and that his sensitive medical information will be disclosed.

Sara Jean Williams

115. Plaintiff Sara Jean Williams is a resident and citizen of Missouri.

116. Plaintiff Williams receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

117. Plaintiff Williams received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Williams' name, address, telephone number, date of birth, gender, health plan subscriber ID number, and Medicare number. Plaintiff Williams has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

118. Plaintiff Williams is highly concerned that her Private Information is now in unknown hands and is fearful that her Private Information is being, and will continue to be, misused. Before the Data Breach occurred, Plaintiff Williams did not receive spam calls, but since the Data Breach occurred, she has experienced a large number of spam calls. Plaintiff Williams is anxious and fearful that he will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

Wanda Wilson

119. Plaintiff Wanda Wilson is a resident and citizen of Texas.

120. Plaintiff Wilson receives benefits from NationsBenefits by virtue of her health plan membership with Aetna.

121. Plaintiff Wilson received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Wilson's name, address, telephone number, date of birth, gender, health plan subscriber ID number, and Medicare

number. Plaintiff has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

122. Plaintiff Wilson was the victim of identity theft following the Data Breach. After the Data Breach, unauthorized charges began appearing on Plaintiff Wilson's debit card, forcing her to spend approximately 45 minutes on the phone with her bank to address the fraudulent charges and to close her bank account and open a new account. Plaintiff Wilson was charged approximately \$300 for late or failed payments as a result of changing her billing information due to the Data Breach. She has received telephone calls regarding account inquiries, and her credit score has decreased since the Data Breach. Plaintiff Wilson has also experienced an increased number of spam calls, texts, and emails since the Data Breach. Plaintiff Wilson spent approximately \$24.95 to obtain her credit report after the Data Breach. She has spent approximately 2 hours monitoring her accounts and credit report for other fraudulent charges or accounts. The Data Breach and resulting identity theft have caused Plaintiff Wilson to experience frustration and anxiety, and she fears that her insurance coverage will be affected.

Stephen Wolsey

123. Plaintiff Stephen Wolsey is a resident and citizen of Florida.

124. Plaintiff Wolsey receives benefits from NationsBenefits by virtue of his health plan membership with Aetna.

125. Plaintiff Wolsey received a letter from NationsBenefits dated April 27, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of NationsBenefits. According to the letter, the compromised files contained Plaintiff Wolsey's first name, middle initial, last name, gender, address, telephone number, date of birth, and health plan subscriber ID number, and other items relating to Plaintiff Stephen Wolsey's receipt of benefits from

NationsBenefits. Plaintiff Stephen Wolsey has faced, and faces a present and continuing risk of fraud and identity theft for his lifetime.

126. As a result of the Data Breach, Plaintiff Wolsey has experienced four fraudulent attempts of opening credit cards with Chase Bank by an unauthorized person. Additionally, Plaintiff Wolsey has noticed an increase phishing attempts in text messages requesting he “click the link below,” and spam phone calls asking him to press a number to continue. Plaintiff Wolsey is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

B. Defendants

127. Defendant NationsBenefits LLC is a Florida limited liability company headquartered in Plantation, Florida. Its sole member is Glenn Parker, a Florida resident and citizen.

128. Defendant NationsBenefits Holdings LLC is a Delaware limited liability company that on information and belief is also headquartered in Plantation, Florida. On information and belief, its sole member is also Glenn Parker, a Florida resident and citizen.

129. NationsBenefits provides supplemental benefits administration services to employers, health insurance companies, and other entities’ health plans. It serves “millions” of members as a “leading provider of supplemental benefits, flex cards, and member engagement solutions that partners with managed care organizations to provide innovative healthcare solutions designed to drive growth, improve outcomes, reduce costs, and delight members.”⁴

⁴ See *About Us*, NATIONS BENEFITS, <https://www.nationsbenefits.com/about-us> (last visited Aug. 22, 2023).

III. FACTUAL ALLEGATIONS

A. NationsBenefits Collects and Uses Personal and Sensitive Customer Data.

130. NationsBenefits is one of the fastest-growing supplemental benefits administration companies in the United States, which provides its services to health insurance plans and employers across the country. Founded in 2015 as “Nation’s Hearing,” NationsBenefits now provides an array of supplemental healthcare solutions, including:

- a. NationsBenefits, which provides hearing benefits, such as digital hearing tests, annual hearing tests, and coverage for hearing aids or related technologies;
- b. NationsOTC, which provides benefits administration and an e-commerce platform for over-the-counter health items, such as foods, first-aid supplies, and other health and wellness items;⁵
- c. NationsMarket, which provides benefits administration for purchasing healthy foods, including prepared meals, fresh produce, and groceries;
- d. NationsCare, which is a companion care benefit, which provides a Companion to members for non-medical assistance such as emotional support, household chores, errands, and transportation;⁶
- e. A Personal Emergency Response Systems benefit, which includes in-home Medical Alert base units, help buttons, GPS monitoring, and other monitoring for elderly members;⁷ and
- f. Connectivity devices, such as tablets, fitness trackers, and phones, for elderly members.⁸

131. It also provides customer experience services for insurance plans, leveraging data analytics to increase member engagement and satisfaction.⁹

⁵ See *NationsOTC*, NATIONS BENEFITS, <https://www.nationsbenefits.com/nationsotc> (last visited Aug. 22, 2023).

⁶ See *Optimized Companion Care Benefit*, NATIONS BENEFITS, <https://www.nationsbenefits.com/Wellness#optimizedcompanioncarebenefit> (last visited Aug. 22, 2023).

⁷ See *Wellness Solutions*, NATIONS BENEFITS, <https://www.nationsbenefits.com/Wellness#pers-benefit> (last visited Aug. 22, 2023).

⁸ See *id.*

⁹ See *NationsCX*, NATIONS BENEFITS, <https://www.nationsbenefits.com/NationsCX> (last visited Aug. 22, 2023).

132. In the last three years, NationsBenefits has experienced incredibly rapid growth, from just 200 employees in 2020 to over 2,500 employees today.¹⁰ According to reports, it has also experienced 868% revenue growth over that time period.¹¹

133. By virtue of its partnerships with other healthcare organizations, NationsBenefits collects and processes an enormous volume of personal data from millions of individuals, including Private Information, including health and patient records and insurance information, geolocation data, and financial information. Much of this information is not provided to NationsBenefits directly, but through insurance providers or employers. Plaintiffs and Class Members whose insurance or managed care organizations partner with NationsBenefits are often required to share their sensitive Private Information with NationsBenefits in order to receive the member benefits to which they are entitled.

134. NationsBenefits strongly urges—or even requires—its clients, users, and patients to provide Private Information to leverage any of its products and services. NationsBenefits explicitly warns customers those certain services “may require you to provide Private Information.”¹² In addition, to distinguish itself from other competitors in the supplemental benefits market, NationsBenefits highlights its data collection and analytics, including analyzing past and present clinical health plan data to “assess known and unknown member needs.”

135. One method of direct information collection occurs on its membership platform, the MyBenefits Portal, where members fill out a personal health profile, including sensitive information

¹⁰ *Compare A Family Tragedy Changed This Founder's Business Philosophy. Now He Has the Fastest-Growing Company in Florida*, INC.COM, <https://www.inc.com/cameron-albert-deitch/inc5000-florida-series-nationsbenefits-health-insurance.html> (“NationsBenefits has grown to 200 full-time employees”) *with Who We Are*, NATIONS BENEFITS, <https://www.nationsbenefits.com/about-us> (“With more than 2,500 employees across all locations . . .”).

¹¹ *See Company Profile—No. 681 NationsBenefits*, INC.COM, <https://www.inc.com/profile/nationsbenefits> (last visited Aug. 22, 2023).

¹² *See Privacy Policy*, NATIONS BENEFITS, <https://nationsbenefits.com/privacy> (last visited Aug. 22, 2023).

about current health concerns, and can purchase goods and services with their supplemental benefits. Members can also schedule appointments with recommended doctors through this platform and share medical records with providers. Use of these portals by individuals such as Plaintiffs and the Class are often required for them to obtain certain benefits, such as purchasing products online with plan benefit dollars.

136. Another example of such collection arises from the use of NationsBenefits OTC mobile app, which allows individuals to use their health insurance or benefit plans “to purchase medications, health and wellness items, and first aid supplies with home delivery at no additional cost.”¹³

137. In its Privacy Policy, NationsBenefits promises customers that it will “use reasonable physical, technical, and administrative safeguards” to protect customers’ Private Information.¹⁴

138. It also promises customers that it will only share customer information in limited circumstances, none of which include sharing with the cyber criminals that facilitated the Data Breach.¹⁵

139. Notably, the Privacy Policy does not disclose that third parties, who may be reckless and/or negligent, will collect, process, and store PHI protected under HIPAA.

140. Plaintiffs and Class Members relied on NationsBenefits’ promise to keep their Private Information confidential and securely maintained, and to only make authorized disclosures of this information. NationsBenefits failed to do so.

¹³ See *Technology*, NATIONS BENEFITS, <https://nationsbenefits.com/technology#mobile-apps> (last visited Aug. 22, 2023).

¹⁴ See *Privacy Policy*, NATIONS BENEFITS, *supra* n.12.

¹⁵ *Id.*

141. Plaintiffs and Class Members also relied on NationsBenefits to ensure that it held vendors with whom it shared sensitive Private Information to the same high standards of data protection. NationsBenefits failed to do so.

B. NationsBenefits Partnered with Fortra for File Transfer Services and Data Storage.

142. To facilitate sharing of sensitive patient information between NationsBenefits, its insurance provider and employer clients, and healthcare providers, NationsBenefits purchased and used a managed file transfer software from Fortra: GoAnywhere MFT.

143. GoAnywhere MFT “is a managed file transfer solution that automates and secures file transfers using a centralized enterprise-level approach.”¹⁶ It acts as a “central point of administration” between an organization’s internal organization, external partners and clients, appliances, and cloud environments.¹⁷ It allegedly includes “extensive security controls” and “automatic encryption” that may be customized for each organization.¹⁸ Fortra promised that GoAnywhere MFT “will provide a safe, audited method for automatically transferring information in and outside of your enterprise.”¹⁹

144. On information and belief, the default settings for GoAnywhere MFT are not compliant with reasonable security standards. The GoAnywhere MFT installation guide provides instructions for how to make the product more secure.

145. For example, the default configuration of GoAnywhere MFT allows anyone with access to the internet to view the landing page, or “administrative console” for a client’s GoAnywhere MFT, where users can sign in to access, operate, and modify the program.²⁰ Fortra’s instructions

¹⁶ *Start Using GoAnywhere MFT*, FORTA, <https://www.goanywhere.com/offers/start-using-mft> (last visited Aug. 22, 2023).

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *GoAnywhere MFT Install Guide*, FORTA, https://static.goanywhere.com/guides/ga_installation_guide.pdf (last visited Aug. 22, 2023).

provide several simple steps that limit public access to this console, such as limiting access to specific ports, meaning that only certain users can access an organization's administrative console. Without these changes, GoAnywhere MFT is vulnerable to attack and exploitation, and is not compliant with reasonable security standards and HIPAA requirements.²¹

146. Fortra has also disclosed security vulnerabilities in GoAnywhere MFT in the past, which rendered their software vulnerable to exploitation, which NationsBenefits knew or should have known.²²

147. Upon information and belief, NationsBenefits was able to control the security and configurations of the MFT servers that stored Class Members' sensitive information for transfer, and were responsible for protecting, maintaining, and monitoring those servers for threat activity.

148. Upon information and belief, NationsBenefits did not change the default settings on its installation of GoAnywhere MFT, including leaving the administrative console exposed to anyone with internet access, failing to comply with reasonable security standards and HIPAA requirements.

C. NationsBenefits Allowed the Private Information of Plaintiffs and Class Members to be Compromised in the Data Breach.

149. Between January 28, 2023, and January 30, 2023, Clop accessed NationsBenefits' servers through a vulnerability in the GoAnywhere MFT administrative console.

150. Over 130 organizations, including several healthcare organizations, were affected by data breaches stemming from this attack.²³

²¹ Dave Shackelford, *Web-Based Admin Consoles: The Critical, Overlooked Security Exposure you must Address*, BEYONDTRUST (Aug. 10, 2021), <https://www.beyondtrust.com/blog/entry/web-based-admin-consoles-the-critical-overlooked-security-exposure-you-must-address>.

²² Fortra, *GoAnywhere MFT Security Advisory*, <https://www.goanywhere.com/support/advisory/68x> (last visited Aug. 22, 2023).

²³ Danny Wimmer, *Fortra Data Breach Targets 130 Companies, Many in Healthcare Sector*, MICH. DEP'T OF ATT'Y GEN. (May 16, 2023), <https://www.michigan.gov/ag/news/press-releases/2023/05/16/fortra-data-breach-targets-130-companies-many-in-healthcare-sector>.

151. Even though similar vulnerabilities in administrative consoles are a common method of exploitation, NationsBenefits did not prevent the attack.

152. This vulnerability, assigned the number CVE-2023-0669 by the National Institute of Standards and Technology (“NIST”), is only accessible to attackers where the GoAnywhere MFT administrator console is publicly accessible through the internet, as was the case with NationsBenefits’ MFT.²⁴

153. The vulnerability allowed the hackers to take the following actions on NationsBenefits’ servers:

- a. Create unauthorized user accounts and download files from MFT servers; and
- b. Install two tools, “Netcat”²⁵ and “Errors.jsp”²⁶ which enabled the hackers to exfiltrate data and establish “backdoors” into the breached system, which allow them to access more data and re-enter the breached systems at later dates.

154. Upon information and belief, these actions enabled the hackers not only to access and download NationsBenefits’ customers’ sensitive Private Information, but also to move across NationsBenefits’ other networks and systems to access vast troves of Private Information.

155. Upon information and belief, Clop issued a ransom demand to NationsBenefits and threatened to leak customer data unless paid. The hackers claimed to have acquired “Customer

²⁴ Caitlin Condon, *Exploitation of GOAnywhere MFT zero-day vulnerability*, RAPID7 (May 4, 2023), <https://www.rapid7.com/blog/post/2023/02/03/exploitation-of-goanywhere-mft-zero-day-vulnerability>.

²⁵ Bill Toulas, *Fortra shares findings on GoAnywhere MFT zero-day attacks*, BLEEPINGCOMPUTER (April 19, 2023), <https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/> (Netcat is “is a versatile networking utility that threat actors typically use to establish backdoors, conduct port scanning, or transfer files between the compromised system and their server.”).

²⁶ *Id.* (“Errors.jsp is a JavaServer Pages (JSP) file used for creating dynamic web pages. Fortra does not explain how the attackers used the file. However, it’s possible that it was designed to provide the attacker with a web-based backdoor on the breached system for executing commands, stealing data, or maintaining access to the environment.”).

databases: name, address, phone number, date of birth, gender, marital status, insurance company name and address. [L]ogs and backups of the production server,” and released the data in five parts.²⁷

156. Upon information and belief, Clop has already posted and/or sold Plaintiffs’ and Class Members’ sensitive information on their dark web-based store, known as “Clop Leaks.”²⁸

157. In a statement, the hackers claimed that they could access other parts of victim’s networks and systems and deploy malware, “but decided against it and only stole the documents stored on the compromised GoAnywhere MFT servers.”²⁹

158. Upon information and belief, other cybercriminal groups and attackers leveraged this exploitation alongside Clop.³⁰

159. Upon information and belief, Plaintiffs’ and Class Members’ Private Information was accessible, unprotected, unencrypted, and therefore easily accessible for unauthorized access and exfiltration.

D. NationsBenefits’ Delay in Securing its Systems and Notifying its Customers of the Data Breach Caused Harm to Plaintiffs and Class Members.

160. Although NationsBenefits was compromised between January 28, 2023, and January 30, 2023, it did not recognize that its servers had been hacked for at least nine more days.³¹ And even though Fortra notified its enterprise customers, including NationsBenefits, of the exploit on February

²⁷ *The Fortra/GoAnywhere breach also affected healthcare entities. Here’s what we know so far*, DATABREACHES.NET (April 21, 2023), <https://www.databreaches.net/the-fortra-goanywhere-breach-also-affected-healthcare-entities-heres-what-we-know-so-far/>

²⁸ *Id.*

²⁹ Sergui Gatlan, *Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day*, BLEEPINGCOMPUTER (Feb. 10, 2023), <https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day>.

³⁰ Ido Lev, *BlackCat / Alphy Ransomware Group Exploits GoAnywhere Vulnerability (CVE-2023-0669) With Higher-Than-Average Demands*, AT BAY (Apr. 25, 2023), <https://www.atbay.com/articles/blackcat-ransomware-group-exploits-goanywhere-vulnerability>.

³¹ Steve Adler, *NationsBenefits Holdings Confirms 3 Million Record Data Breach*, THE HIPAA JOURNAL (May 8, 2023), <https://www.hipaajournal.com/nationsbenefits-holdings-confirms-3-million-record-data-breach>.

3, 2023, providing details of the exploit, indicators of compromise, and mitigation options.³² NationsBenefits did not take steps to secure their servers until much later.

161. Indeed, the length of time the Data Breach went unnoticed and undetected by NationsBenefits is astonishing. Security researchers and news outlets quickly disseminated the warning *en masse*. As of February 4, 2023, media outlets Security Affairs and the Hacker News released detailed articles detailing that the exploits were being leveraged by malicious actors and providing potential mitigation steps that companies could take to prevent exploitation.³³

162. Upon information and belief, NationsBenefits failed to update its systems to include the indicators of compromise or make any mitigation efforts until February 7, 2023, leaving their systems unprotected and open for exploitation for over a week.

163. On April 13, 2023, more than two months after it discovered the theft of its customers' highly sensitive information, NationsBenefits notified the United States Department of Health and Human Services that 3,037,303 individuals were affected by the Data Breach.³⁴

164. NationsBenefits also waited more than two months after it discovered its customers' Private Information had been stolen before sending notices to individuals whose data was stolen in the Data Breach. While NationsBenefits first sent notices to impacted individuals on April 13, 2023, letters to some Plaintiffs were not sent until April 27, 2023, and even later. The notice stated the following:

³² Sergui Gatlan, *Exploit released for actively exploited GoAnywhere MFT zero-day*, BLEEPINGCOMPUTER (Feb. 6, 2023), <https://www.bleepingcomputer.com/news/security/exploit-released-for-actively-exploited-goanywhere-mft-zero-day>.

³³ See Pierluigi Paganini, *GoAnywhere MFT zero-day flaw actively exploited*, SECURITY AFFAIRS (Feb. 4, 2023), <https://securityaffairs.com/141826/hacking/goanywhere-mft-zero-day.html> (last visited Aug. 22, 2023); Ravie Lakshmanan, *Warning: Hackers Actively Exploiting Zero-Day in Fortra's GoAnywhere MFT*, THE HACKER NEWS (Feb. 4, 2023), <https://thehackernews.com/2023/02/warning-hackers-actively-exploiting.html>).

³⁴ U.S. Department of Health and Human Services, *Cases Currently Under Investigations*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Aug. 22, 2023).

What Happened? NationsBenefits used software provided by a third-party vendor, Fortra, LLC (“Fortra”), to securely exchange files with your health plan. On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations, including NationsBenefits. When we learned of this incident on February 7, 2023, we immediately took steps to secure our systems and launched an investigation, which was conducted by an experienced outside law firm and a leading cybersecurity firm. As part of our investigation, NationsBenefits analyzed the impacted data to determine whether any individual’s Private Information was subject to unauthorized access or acquisition. On February 23, 2023, NationsBenefits confirmed that, unfortunately, some of your Private Information was affected by the incident.

What Information Was Involved? The Private Information involved included your First Name; Middle Initial; Last Name; Gender; Health Plan Subscriber Identification Number; Address; Date of Birth; Medicare number.³⁵

165. NationsBenefits did not mention that the Clop hackers very likely stole even more information from its systems, including Social Security numbers, full names, and phone numbers. Given the sensitive information stored on NationsBenefits’ servers, other data that may have been stolen included medical records, financial information, and geolocation information. Due to the high level of access that the attackers had to NationsBenefits’ servers, this additional information was likely exposed for exfiltration and stolen.

166. NationsBenefits’ notice letter also omitted the size and scope of the Data Breach. Nor did NationsBenefits’ notice letter identify the ransomware used, or what steps NationsBenefits intends to take to enhance its data security systems and monitoring capabilities to prevent further breaches. Although NationsBenefits claimed to have stopped its usage of GoAnywhere MFT, it did not provide any assurances that it would improve its data security practices with other file transfer services. Without changes to NationsBenefits’ own practices, Plaintiffs’ and Class Members’ sensitive information remains at risk, regardless of the specific file transfer service that NationsBenefits uses.

³⁵ See Ex. A.

167. NationsBenefits' inadequate communications have left Plaintiffs and Class Members in the dark regarding the extent of the harm they have suffered, and NationsBenefits has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

E. NationsBenefits Knew It Was a Likely Target of a Cyberattack.

168. At all relevant times, NationsBenefits was aware, or reasonably should have been aware, that the Private Information collected, maintained, and stored in their servers is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties, such as identity theft, medical identity theft, fraud and other misuse.

169. File transfer services like GoAnywhere MFT are popular and well-known targets for cyberattacks. Some of the largest healthcare data breaches in recent history occurred by cyber criminals targeting file transfer services. For example, in February 2021, the file transfer service Accellion was attacked by the same threat actors as the Data Breach (Clop) causing the theft of more than three million patients' information.³⁶

170. Indeed, NationsBenefits knew or should have known that services from third-party vendors like Fortra were frequently attacked, leading to ninety percent of healthcare-related cyberattacks in 2021 and 2022.³⁷

³⁶ Ionut Ilascu, *Global Accellion data breaches linked to Clop ransomware gang*, BLEEPINGCOMPUTER (Feb. 22, 2021), <https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/>; *Exploitation of Accellion File Transfer Appliance*, CYBERSECURITY INFRASTRUCTURE & SECURITY AGENCY (June 17, 2021), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-055a>.

³⁷ Jessica Davis, *Most of the 10 largest healthcare data breaches in 2022 are tied to vendors*, SC MEDIA (Dec. 12, 2022), <https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-vendors>; Jessica Davis, *Vendor incidents lead the 10 biggest health care data breaches of 2021 so far*, SC MEDIA (June 30, 2021), <https://www.scmagazine.com/news/risk-management/vendor-incidents-lead-the-10-biggest-health-care-data-breaches-of-2021-so-far>.

171. The frequency and prevalence of attacks make it imperative for entities to monitor for exploits and attacks routinely and constantly, and regularly update their software and security procedures.

172. NationsBenefits was fully aware that the healthcare benefits industry is a prime target for cyber threats.³⁸ High profile data breaches in for similar industry leaders in healthcare put them on notice of this fact, *e.g.*, Trinity Health (3.3 million patients, May 2020); Shields Healthcare Group (2 million patients, March 2022). Between 2020 and 2021, attacks on the healthcare industry increased 71%, making it the fifth most common industry targeted by cyberattacks.³⁹

173. NationsBenefits also knew or should have known of the threat that Clop posed to their patients. The healthcare industry is also the primary target of Clop.⁴⁰ The Department of Health and Human Services even issued alerts in 2021 and early January 2023 warning the healthcare sector of potential Clop attacks.⁴¹ Clop has previously targeted file transfer services as a means to target the healthcare sector.⁴²

F. NationsBenefits Breached Its Duties to Plaintiffs and Class Members.

174. As an entity collecting, maintaining, and profiting off Plaintiffs' and Class Members' highly sensitive Personal Information, NationsBenefits had a duty to exercise reasonable care and comply with applicable industry standards and statutory security requirements to protect their information.

³⁸ See Finkle, *FBI warns healthcare firms they are targeted by hackers*, *supra* n.3.

³⁹ Check Point Research Team, *Check Point Research: Cyber Attacks Increased 50% Year over Year*, Check Point (Jan. 10, 2022), <https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year>.

⁴⁰ HC3, *Analyst Note: Clop Ransomware*, HHS (Jan. 4, 2023), <https://www.hhs.gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf>.

⁴¹ *Id.*

⁴² HC3, *Analyst Note: CLOP Poses Ongoing Risk to HPH Organizations*, HHS (Mar. 23, 2021), <https://www.hhs.gov/sites/default/files/clop-poses-ongoing-risk-to-hph-organizations.pdf>.

175. Indeed, NationsBenefits was on notice that it was maintaining highly valuable data, which it knew was at risk of being targeted by cybercriminals, and knew of the extensive harm that would occur if Plaintiffs' and Class Members' Private Information was exposed through a data breach.

176. Because Plaintiffs and Class Members provided their Private Information to their respective health plans or other entities who in turn provided that information to NationsBenefits, NationsBenefits had a special relationship with Plaintiffs and Class Members which provided an independent duty of care. NationsBenefits owed a duty to use reasonable security measures because it undertook to collect, store, and use customers' Private Information. In addition, NationsBenefits owed a duty to require and ensure that Fortra would use reasonable security measures because it disclosed that same Private Information to Fortra.

177. NationsBenefits' HIPAA Rights disclosure even provides that it is "required by law to maintain the privacy and security of your protected health information."⁴³

178. In that same HIPAA Rights disclosure, NationsBenefits told its customers: "We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."⁴⁴

179. Despite holding Private Information for millions of individuals, NationsBenefits failed to adopt reasonable data security measures to prevent and detect unauthorized access to their highly sensitive databases, putting their customers' highly sensitive information at risk.

180. NationsBenefits failed to properly implement data security practices that were reasonable and up to industry standards.

⁴³ *Your HIPAA Rights*, NATIONS BENEFITS, <https://www.nationsbenefits.com/hipaa> (last visited Aug. 22, 2023).

⁴⁴ *Id.*

G. NationsBenefits Failed to Comply with Regulatory Requirements and Industry Practices.

181. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

182. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain Private Information, about a resident of that state to implement and maintain “reasonable security procedures and practices” and to protect Private Information from unauthorized access. Florida is one such state and requires that entities like NationsBenefits “take reasonable measures to protect and secure data in electronic form containing personal information.” Fla. Stat. § 501.171(2).

183. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.⁴⁵

184. The Federal Trade Commission (“FTC”) has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁴⁶

⁴⁵ See *Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), <https://insights.datamark.net/addressing-bpo-information-security> [<https://perma.cc/NY6X-FUY>].

⁴⁶ *Start With Security*, FED. TRADE COMM’N, at 2, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Aug. 22, 2023).

185. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.⁴⁷ The guidelines note businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

186. The FTC also recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.⁴⁸

187. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

⁴⁷ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 22, 2023).

⁴⁸ *See Start With Security*, FED. TRADE COMM'N, *supra* n.48.

188. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information⁴⁹ and failure to segregate access to information⁵⁰ may violate the FTC Act.

189. NationsBenefits' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (*i.e.*, Private Information) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

190. Furthermore, NationsBenefits is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

191. The Security Rule requires NationsBenefits to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

⁴⁹ *In the Matter of LabMD, Inc.*, Dkt. No. 9357, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), <https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf>.

⁵⁰ *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (stating that companies should use "readily available security measures to limit access between" data storage systems).

- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.⁵¹

192. Pursuant to HIPAA's mandate that NationsBenefits follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302. NationsBenefits was required to, at minimum, to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

193. NationsBenefits is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

194. Both HIPAA and HITECH obligate NationsBenefits to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

195. As alleged in this Complaint, NationsBenefits has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of protected health information.

⁵¹ *Summary of the HIPAA Security Rule*, HHS, <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> (last visited Aug. 22, 2023).

196. Additionally, cybersecurity experts have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.⁵² NationsBenefits did not follow such minimum best practices.

H. The Data Breach Harmed Plaintiffs and Class Members.

197. NationsBenefits' failure to keep Plaintiffs' and Class Members' Private Information secure has had severe ramifications, examples of which are alleged above for the Plaintiffs. Given the sensitive nature of the information stolen in the Data Breach—names, Social Security numbers, birthdates, addresses, health information—hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

198. This data is highly coveted and valuable on underground or black markets. Upon information and belief, Plaintiffs' and Class Members' data has already been leaked and sold on the black market.

199. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even

⁵² See *Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), <https://insights.datamark.net/addressing-bpo-information-security/> [<https://perma.cc/NY6X-TFUY>].

undergo surgery under a false identity.⁵³ The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their Medicare numbers, health insurance information, or Social Security numbers.

200. Medicare beneficiary numbers like Plaintiffs’ are “even more valuable than stolen credit cards,” and often result in the filing of false claims for Medicare reimbursement.⁵⁴

201. According to the U.S. Government Accountability Office, “stolen data may be held for up to a year or more before being used to commit identity theft,” and “once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.”⁵⁵

202. Because of its value and the loss of sensitive health information and Social Security numbers, future identity theft is imminently and certainly impending.

203. The exposure of any Private Information can cause unexpected harms one would not ordinarily associate with the type of information stolen. Cybercriminals routinely aggregate Private Information from multiple illicit sources and use stolen information to gather even more information through social engineering, credential stuffing, and other methods. The resulting complete dossiers of Private Information are particularly prized among cybercriminals because they expose the target to every manner of identity theft and fraud.

204. Identity thieves can use Private Information such as that exposed in the Data Breach to: (a) apply for credit cards or loans (b) purchase prescription drugs or other medical services (c)

⁵³ *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, FTC, <https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf> (last visited Aug. 22, 2023).

⁵⁴ Melissa D. Berry, *Medicare under attack: Healthcare data breaches increase fraud risks*, THOMSON REUTERS (Mar. 3, 2023), <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/medicare-fraud-risks>.

⁵⁵ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, U.S. GOV’T ACCOUNTABILITY OFF., 42 (June 2007), <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07737/html/GAOREPORTSGAO-07-737.htm> (last visited Aug. 22, 2023).

commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

205. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole \$16.8 billion from consumers in the United States, which includes \$5.1 billion stolen through bank account take-overs.⁵⁶

206. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is \$445 billion a year.⁵⁷

207. For Plaintiffs and Class Members who had their Social Security numbers exposed, the unauthorized disclosure can be particularly damaging because, unlike a credit card, Social Security numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other Private Information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other Private Information, such as your name and address, remains the same.

⁵⁶ *2018 Identity fraud: Fraud Enters a New Era of Complexity*, JAVELIN, <https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity> (last visited Aug. 22, 2023).

⁵⁷ *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last visited Aug. 22, 2023).

If you receive a new Social Security number, you shouldn't use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.⁵⁸

208. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a Social Security number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

209. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages.⁵⁹ For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

210. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

211. The 2017 Identity Theft Resource Center survey⁶⁰ evidences the emotional suffering experienced by victims of identity theft:

⁵⁸ *Identity Theft and Your Social Security number*, SOCIAL SECURITY ADMINISTRATION, <http://www.ssa.gov/pubs/10064.html> (last visited Aug. 22, 2023).

⁵⁹ *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Aug. 22, 2023).

⁶⁰ *Id.*

- 75% of respondents reported feeling severely distressed.
- 67% reported anxiety.
- 66% reported feelings of fear related to personal financial safety.
- 37% reported fearing for the financial safety of family members.
- 24% reported fear for their physical safety.
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft.
- 7% reported feeling suicidal.

212. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances.
- 37.1% reported an inability to concentrate / lack of focus.
- 28.7% reported they were unable to go to work because of physical symptoms.
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues).
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.⁶¹

213. There may also be a significant time lag between when Private Information is stolen and when it is actually misused. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁶²

⁶¹ *Id.*

⁶² *See, Report to Congressional Requesters*, U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* n.1.

214. As the result of the Data Breach, Plaintiffs and Class Members have suffered and/or will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- losing the inherent value of their Private Information;
- losing the value of NationsBenefits' implicit promises of adequate data security;
- identity theft and fraud resulting from the theft of their Private Information;
- costs associated with the detection and prevention of identity theft and unauthorized use of their medical and health insurance information;
- costs associated with purchasing credit monitoring and identity theft protection services;
- unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

- the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being in the possession of one or many unauthorized third parties.

215. Additionally, Plaintiffs and Class Members place significant value in data security.

216. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like NationsBenefits would have no reason to tout their data security efforts to their actual and potential customers.

217. Consequently, had customers including Plaintiffs and Class Members known the truth about NationsBenefits' data security practices—that the company would not adequately protect and store their data—they would not have entrusted their Private Information to their respective health plans or other entities to then transfer to Nations Benefits, purchased health benefits that included NationsBenefits' services, or paid as much for such services or benefits. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with NationsBenefits because they paid for a value of services they expected but did not receive.

218. When NationsBenefits announced the Data Breach to its customers, it deliberately underplayed the Data Breach's severity, obfuscated the nature of the Data Breach and offered only de minimis relief. NationsBenefits merely advised its customers to “remain vigilant for incidents of fraud and identity theft” and suggested they: order a free credit report; contact the FTC and/or state attorney general's office for more information on how to prevent or avoid identity theft; place a security freeze or fraud alert; and offered 24 months of credit monitoring. Not only are each of these suggestions

steps that Plaintiffs and Class Members must take on their own free time, but they do not come close to compensating Plaintiffs and the Class for the lifetime risks they face.⁶³

219. Plaintiffs themselves suffered incidences of harm, including identity theft, which are alleged in detail in Section **Error! Reference source not found.**, *supra*.

IV. CLASS ACTION ALLEGATIONS

220. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as appropriate, and (c)(4), Plaintiffs seek certification of the following nationwide class (the “Class” or the “Nationwide Class”):

Nationwide Class

All persons in the United States whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

221. The Nationwide Class asserts claims against NationsBenefits for negligence (Count I); negligence per se (Count II); breach of third-party beneficiary contract (Count III); breach of implied contract (Count IV); unjust enrichment (Count V); and for declaratory and injunctive relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.* (Count VI).

222. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as appropriate, and (c)(4), Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts VII through XXVII) on behalf of subclasses for residents of Arkansas, California, Florida, Illinois, Indiana, Kansas, Michigan, Missouri, New Jersey, New York, North Carolina, Ohio, Pennsylvania, and Texas (collectively “State Subclasses” or individually “State Subclass”). Each State Subclass is defined as follows:

⁶³ See Ex. A [or <https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-187.pdf>].

Arkansas Subclass

All residents of Arkansas whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

California Subclass

All residents of California whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Florida Subclass

All residents of Florida whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Illinois Subclass

All residents of Illinois whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Indiana Subclass

All residents of Indiana whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Kansas Subclass

All residents of Kansas whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Michigan Subclass

All residents of Michigan whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Missouri Subclass

All residents of Missouri whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

New Jersey Subclass

All residents of New Jersey whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

New York Subclass

All residents in New York whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

North Carolina Subclass

All residents in North Carolina whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Ohio Subclass

All residents in Ohio whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Pennsylvania Subclass

All residents in Pennsylvania whose Private Information was compromised in the data breach announced by NationsBenefits on April 13, 2023.

Texas Subclass

All residents in Texas whose Private Information was compromised the data breach announced by NationsBenefits on April 13, 2023.

223. Excluded from the Nationwide Class and the State Subclasses (collectively, the “Classes”) are NationsBenefits, any entity in which NationsBenefits has a controlling interest, and NationsBenefits’ officers, directors, legal representatives, successors, subsidiaries, and assigns; all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; any judicial officer presiding over any aspect of this matter, members of their immediate family, and members of their judicial staff; any individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; Plaintiffs’ counsel and NationsBenefits’ counsel; members of the jury; and the legal representatives.

224. Plaintiffs hereby reserve the right to amend or modify the Class definitions with greater specificity or division after having had an opportunity to conduct discovery.

225. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Classes are so numerous and geographically dispersed that the joinder of all members is impractical.

While the exact number of Class Members is unknown to Plaintiffs at this time, NationsBenefits has acknowledged that the Private Information of approximately 3,037,303 individuals throughout the United States was compromised in the Data Breach. Those persons' names and addresses are available from NationsBenefits' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice. Upon information and belief, there are at least thousands of members in each State Subclass, making joinder of all State Subclass Members impractical.

226. Predominance of Common Issues. Fed. R. Civ. P. 23(a)(2) and (b)(3).

Consistent with Rule 23(a)(2)'s commonality requirement and Rule 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

- a. Whether NationsBenefits unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b. Whether NationsBenefits' conduct violated the FTC Act and/or HIPAA;
- c. Whether NationsBenefits' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including HIPAA and HITECH;
- d. Whether NationsBenefits' data security systems were consistent with industry standards;
- e. Whether NationsBenefits knew or should have known that its GoAnywhere MFT servers and configurations were vulnerable to attack;
- f. Whether NationsBenefits failed to take adequate and reasonable measures to ensure that its computer, applications, and data systems were protected and updated;

- g. Whether NationsBenefits failed to take available steps to prevent and stop the Data Breach from happening;
- h. Whether NationsBenefits should have discovered the data breach earlier;
- i. Whether NationsBenefits took reasonable measures to determine the extent of the Data Breach after it was discovered;
- j. Whether NationsBenefits owed tort duties to Plaintiffs and Class Members to protect their Private Information;
- k. Whether NationsBenefits owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- l. Whether NationsBenefits' delay in informing Plaintiffs and Class Members of the Data Breach was unreasonable;
- m. Whether NationsBenefits' method of informing Plaintiffs and Class Members of the Data Breach was unreasonable;
- n. Whether NationsBenefits breached their duties to protect the Private Information of Plaintiffs and Class Members by failing to provide adequate data security;
- o. Whether NationsBenefits' failure to secure Plaintiffs' and Class Members' Private Information in the manner alleged violated federal, state and local laws, and/or industry standards;
- p. Whether NationsBenefits' conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiffs' and Class Members' Private Information;
- q. Whether NationsBenefits has an implied contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

- r. Whether NationsBenefits' conduct amounted to violations of state consumer protection statutes, including the Arkansas Deceptive Trade Practices Act; California Consumer Privacy Act; California Customer Records Act; California Unfair Competition Act; Florida Deceptive and Unfair Trade Practices Act; Illinois Personal Information Protection Act; Illinois Consumer Fraud and Deceptive Business Practices Act; Illinois Uniform Deceptive Trade Practices Act; Indiana Deceptive Consumer Sales Act; Kansas Protection of Consumer Information Act; Kansas Consumer Protection Act; Michigan Consumer Protection Act; Missouri Merchandise Practices Act; New Jersey Consumer Fraud Act; New York General Business Law § 349; North Carolina Identity Theft Protection Act; North Carolina Unfair Trade Practices Act; Ohio Consumer Sales Practices Act; Ohio Deceptive Trade Practices Act; Pennsylvania Unfair Trade Practices and Consumer Protection Law; and Texas Deceptive Trade Practices—Consumer Protection Act.
- s. Whether, as a result of NationsBenefits' conduct, Plaintiffs and Class Members face a significant ongoing threat of identity theft, harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;
- t. Whether NationsBenefits should retain the money paid by Plaintiffs and Class Members to protect their Private Information;
- u. Whether NationsBenefits should retain Plaintiffs' and Class Members' valuable Private Information; and
- v. Whether, as a result of NationsBenefits' conduct, Plaintiffs and Class Members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

227. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to each of the Classes, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiffs' Private Information was in

NationsBenefits' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seek relief consistent with the relief of the Classes.

228. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Classes because Plaintiffs are each members of the Nationwide Class, and respectively members of the State Subclasses, and are committed to pursuing this matter against NationsBenefits to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of all the Classes.

229. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiffs and Class Members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against NationsBenefits, and thus, individual litigation to redress NationsBenefits' wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

230. **Manageability. Fed. R. Civ. P. 23(b)(3).** The litigation of the class claims alleged herein is manageable. NationsBenefits' uniform conduct, the consistent provisions of the relevant

laws, and the ascertainable identities of Class Members demonstrates there would be no significant manageability problems with prosecuting this lawsuit as a class action.

231. **Ascertainability.** All members of the proposed Classes are readily ascertainable. The Classes are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Classes. NationsBenefits has access to information regarding which individuals were affected by the Data Breach and has already provided notifications to some of those people. Using this information, the members of the Classes can be identified, and their contact information ascertained for purposes of providing notice to the Classes.

232. **Particular Issues. Fed. R. Civ. P. 23(c)(4).** Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether NationsBenefits owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether NationsBenefits breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether NationsBenefits failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between NationsBenefits on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;
- e. Whether NationsBenefits breached the implied contract;
- f. Whether NationsBenefits breached a third-party beneficiary contract;
- g. Whether NationsBenefits adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

- h. Whether NationsBenefits failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether NationsBenefits engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and,
- j. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and/or injunctive relief as a result of NationsBenefits' wrongful conduct.

233. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2) and (c).** Finally, class certification is also appropriate under Rule 23(b)(2) and (c). NationsBenefits, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole, including:

- a. Order NationsBenefits to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.
- b. Order that, to comply with NationsBenefits' explicit or implicit contractual obligations and duties of care, NationsBenefits must implement and maintain reasonable security and monitoring measures, including, but not limited to:
 - i. prohibiting NationsBenefits from engaging in the wrongful and unlawful acts alleged herein;
 - ii. requiring NationsBenefits to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring NationsBenefits to delete and purge the Private Information of Plaintiffs and Class Members unless NationsBenefits can provide to the Court

reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring NationsBenefits to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring NationsBenefits to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on NationsBenefits' systems on a periodic basis;

vi. prohibiting NationsBenefits from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring NationsBenefits to segment data by creating firewalls and access controls so that, if one area of NationsBenefits' network is compromised, hackers cannot gain access to other portions of NationsBenefits' systems;

viii. requiring NationsBenefits to conduct regular database scanning and securing checks;

ix. requiring NationsBenefits to monitor ingress and egress of all network traffic;

x. requiring NationsBenefits to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring NationsBenefits to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with NationsBenefits' policies, programs, and systems for protecting personal identifying information;

xii. requiring NationsBenefits to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor NationsBenefits' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

xiii. requiring NationsBenefits to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xiv. Incidental retrospective relief, including but not limited to restitution.

V. CAUSES OF ACTION

ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF THE STATE SUBCLASSES

COUNT I NEGLIGENCE

234. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

235. NationsBenefits collected sensitive Private Information from Plaintiffs and Class Members as a requirement for using NationsBenefits' products and services.

236. NationsBenefits owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

237. More specifically, this duty included, among other things: (a) regularly designing, maintaining, and testing NationsBenefits' security systems to ensure that Plaintiffs' and Class Members' Private Information in NationsBenefits' possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards, including regularly updating, patching, and evaluating security measures.

238. NationsBenefits' duty to use reasonable care arose from several sources, including but not limited to those alleged herein.

239. NationsBenefits had common law duties to prevent foreseeable harm to Plaintiffs and Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices.

240. NationsBenefits' duty to use reasonable security measures also arose as a result of the special relationship that existed between NationsBenefits, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members provided their valuable PII and sensitive PHI to their respective health plans or other entities who in turn provided that information to NationsBenefits. Only NationsBenefits could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach because it had exclusive knowledge and control regarding same.

241. NationsBenefits admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Private

Information at issue here. Discovery is necessary to fully understand the reasons for this failure, but it appears that in its quest for rapid growth over the last three years, NationsBenefits has failed to put adequate resources and emphasis on the need for data security.

242. NationsBenefits knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential Private Information.

243. NationsBenefits also had a duty to safeguard the Private Information of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require NationsBenefits to reasonably safeguard sensitive Private Information, as detailed herein.

244. Timely, adequate notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles; avoid unauthorized charges to their credit or debit card accounts; cancel or change usernames and passwords on compromised accounts; monitor their account information and credit reports for fraudulent activity; contact their banks or other financial institutions that issue their credit or debit cards; obtain credit monitoring services; contact their health insurers or governmental health insurance providers; and take other steps to mitigate or ameliorate the damages caused by NationsBenefits' misconduct. NationsBenefits was the only entity that had sufficient knowledge to properly provide this notice.

245. NationsBenefits breached the duties it owed to Plaintiffs and Class Members alleged above and, thus, was negligent in failing to do so. NationsBenefits breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Private Information of Plaintiffs and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Private

Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and Class Members' Private Information in NationsBenefits' possession had been or was reasonably believed to have been, stolen or compromised.

246. But for NationsBenefits' wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

247. NationsBenefits' failure to take proper security measures to protect the sensitive Private Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' Private Information.

248. Plaintiffs and Class Members were foreseeable victims of NationsBenefits' inadequate data security practices, and it was also foreseeable that NationsBenefits' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as alleged in this Complaint.

249. As a direct and proximate result of NationsBenefits' negligence, Plaintiffs and Class Members have been injured and are entitled to compensatory and consequential damages suffered because of the Data Breach in an amount to be proven at trial.

250. Such injuries include one or more of the following: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the present and continuing threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their lost work

time; (j) the lost value of the Private Information; (k) the lost value of access to their Private Information permitted by NationsBenefits; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of NationsBenefits' Data Breach; (m) lost benefit of their bargains and overcharges for services or products; and (n) the nominal and general damages and other economic and non-economic harm suffered.

COUNT II
NEGLIGENCE *PER SE*

251. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

252. As alleged above, NationsBenefits had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act.

253. NationsBenefits' violation of HIPAA and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

254. Plaintiffs and Class Members are consumers within the class of persons that HIPAA and Section 5 of the FTC Act were intended to protect.

255. The harm that has occurred is the type of harm HIPAA and the FTC Act were intended to guard against.

256. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

257. NationsBenefits breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

258. In addition, under state data security and consumer protection statutes such as those outlined herein, NationsBenefits had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

259. Plaintiffs and Class Members were foreseeable victims of NationsBenefits' violations of HIPAA, the FTC Act, and state data security and consumer protection statutes. NationsBenefits knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

260. But for NationsBenefits' violations of these applicable laws and regulations, Plaintiffs' and Class Members' Private Information would not have been accessed and exfiltrated by unauthorized cybercriminals.

261. As a direct and proximate result of NationsBenefits' negligence *per se*, Plaintiffs and Members have been injured and are entitled to compensatory and consequential damages suffered because of the Data Breach in an amount to be proven at trial. Such injuries include one or more of the following: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) the mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their lost work time; (j) the lost value of the Private Information; (k) the lost value of access to their Private Information permitted by NationsBenefits; (l)

the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of NationsBenefits' Data Breach; (m) the lost benefit of their bargains and overcharges for services or products; and (n) nominal and general damages; and other economic and non-economic harm.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

262. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

263. On information and belief, NationsBenefits entered into contracts to provide services to its clients, which services included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be provided to it.

264. On information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that NationsBenefits agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

265. NationsBenefits knew that if it were to breach these contracts with its clients, the clients' members, including Plaintiffs and the Class Members, would be harmed.

266. NationsBenefits breached its contracts with its clients—whose members, including Plaintiffs and the Class Members—were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiffs and Class Members regarding the breach.

267. As foreseen, Plaintiffs and the Class Members were harmed by NationsBenefits' failure to use reasonable data security measures to store the Private Information Plaintiffs and Class Members provided to their respective health plans or other entities who in turn provided that information to

NationsBenefits and the failure to timely notify Plaintiffs and Class Members, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

268. Accordingly, Plaintiffs and the Class Members are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

COUNT IV
BREACH OF IMPLIED CONTRACT

269. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

270. NationsBenefits offered to provide services to its clients, which are Plaintiffs' and Class Members' health plan providers, in exchange for payment.

271. NationsBenefits also required Plaintiffs and Class Members to provide it with their Private Information in order to receive services.

272. In turn, NationsBenefits impliedly promised to protect Plaintiffs' and Class Members' Private Information through adequate data security measures.

273. Plaintiffs and Class Members accepted NationsBenefits' offer by providing their valuable PII and sensitive PHI to their respective health plans or other entities who in turn provided that information to NationsBenefits in exchange for Plaintiffs and Class Members receiving NationsBenefits' services, and then by paying for and receiving the same (payments which, upon information and belief, directly benefitted NationsBenefits).

274. Plaintiffs and Class Members would not have done the foregoing but for the above-described agreement with the company.

275. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to NationsBenefits in exchange for, amongst other things, the protection of such information.

276. Plaintiffs and Class Members fully performed their obligations under the implied contracts with NationsBenefits.

277. However, NationsBenefits breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

278. NationsBenefits further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA.

279. NationsBenefits further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information NationsBenefits created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

280. NationsBenefits further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

281. NationsBenefits further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

282. In sum, Plaintiffs and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of NationsBenefits.

283. Moreover, the covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their

terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

284. NationsBenefits' conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

285. As a direct and proximate result of NationsBenefits' above-alleged breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) the mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their lost work time; (j) the lost value of the Private Information; (k) the lost value of access to their Private Information permitted by NationsBenefits; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of NationsBenefits' Data Breach; (m) the lost benefit of their bargains and overcharges for services or products; and (n) nominal and general damages; and other economic and non-economic harm.

286. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

COUNT V
UNJUST ENRICHMENT

287. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

288. This Count is pled in the alternative to Counts III and IV.

289. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, and maintained by NationsBenefits, and that was ultimately stolen in the Data Breach.

290. NationsBenefits benefitted by the conferral upon it of the Private Information pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information. NationsBenefits understood that it so benefitted.

291. NationsBenefits also understood and appreciated that Plaintiffs' and Class Members' Private Information was in fact private and confidential, and its value depended upon NationsBenefits maintaining the privacy and confidentiality of that Private Information.

292. But for NationsBenefits' willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class Members would not have provided their Private Information to their respective health plans or other entities to in turn provide that information to NationsBenefits.

293. Because of its use of Plaintiffs' and Class Members' Private Information, NationsBenefits sold more services and products than it otherwise would have. NationsBenefits was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

294. NationsBenefits also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

295. NationsBenefits further benefited through its unjust conduct in the form of the profits it gained through the use of Plaintiffs' and Class Members' Private Information.

296. The benefits conferred upon, received, and enjoyed by NationsBenefits were not conferred officiously or gratuitously. Under the circumstances, it would be inequitable, unfair, and unjust for NationsBenefits to retain these wrongfully obtained benefits. NationsBenefits' retention of wrongfully obtained monies would also violate fundamental principles of justice, equity, and good conscience.

297. As a result of NationsBenefits' wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiffs and Class Members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), NationsBenefits has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

298. NationsBenefits' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

299. NationsBenefits' defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Private Information and has caused the Plaintiffs and Class Members other damages as alleged herein.

300. Plaintiffs have no adequate remedy at law.

301. NationsBenefits is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on NationsBenefits as a result of its wrongful

conduct, including specifically: (a) the value to NationsBenefits of the Private Information that was stolen in the Data Breach; (b) the profits NationsBenefits received and is receiving from the use of that information; (c) the amounts that NationsBenefits overcharged Plaintiffs and Class Members for use of NationsBenefits' products and services; and (d) the amounts that NationsBenefits should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT VI
DECLARATORY JUDGMENT ACT, 28 U.S.C. §§ 2201 *ET SEQ.*

302. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

303. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

304. NationsBenefits owed a duty of care to Plaintiffs and Class Members, which required it to adequately monitor and safeguard Plaintiffs' and Class Members' Private Information.

305. NationsBenefits still possesses the Private Information belonging to Plaintiffs and Class Members.

306. Plaintiffs allege that NationsBenefits' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

307. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. NationsBenefits owes a legal duty to secure Plaintiffs' and Class Members' Private Information under the common law, HIPAA, the FTCA, the California Medical Information Act, and other state and federal laws and regulations, as set forth herein;

b. NationsBenefits' existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

c. NationsBenefits continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' Private Information.

308. This Court should also issue corresponding prospective injunctive relief requiring NationsBenefits to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, including the following:

c. Order NationsBenefits to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

d. Order that, to comply with NationsBenefits' explicit or implicit contractual obligations and duties of care, NationsBenefits must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. prohibiting NationsBenefits from engaging in the wrongful and unlawful acts alleged herein;

ii. requiring NationsBenefits to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring NationsBenefits to delete and purge the Private Information of Plaintiffs and Class Members unless NationsBenefits can provide to the Court

reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring NationsBenefits to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring NationsBenefits to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on NationsBenefits' systems on a periodic basis;

vi. prohibiting NationsBenefits from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring NationsBenefits to segment data by creating firewalls and access controls so that, if one area of NationsBenefits' network is compromised, hackers cannot gain access to other portions of NationsBenefits' systems;

viii. requiring NationsBenefits to conduct regular database scanning and securing checks;

ix. requiring NationsBenefits to monitor ingress and egress of all network traffic;

x. requiring NationsBenefits to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring NationsBenefits to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with NationsBenefits' policies, programs, and systems for protecting personal identifying information;

xii. requiring NationsBenefits to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor NationsBenefits' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring NationsBenefits to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

309. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of NationsBenefits' systems. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

310. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to NationsBenefits if an injunction is issued., The cost of NationsBenefits' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and NationsBenefits has a pre-existing legal duty to employ such measures.

311. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of

NationsBenefits' systems and network, thus preventing future injury to Plaintiffs and other members whose Private Information would be further compromised.

312. Following the issuance of the declaratory relief requested herein, Plaintiffs and the Class will seek any further necessary or proper relief, including damages, after reasonable notice and hearing, against NationsBenefits.

CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT VII
ARKANSAS DECEPTIVE TRADE PRACTICES ACT
A.C.A. §§ 4-88-101 et seq.

313. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

314. Plaintiffs Pamela Lazaroff and Stephen Lazaroff (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the Arkansas Subclass.

315. NationsBenefits is a "person" as defined by A.C.A. § 4-88-102(5).

316. NationsBenefits' products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

317. NationsBenefits advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

318. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101 *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

319. NationsBenefits engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-108(a)(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-108(a)(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

- a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services or as to whether goods are original or new or of a particular standard, quality, grade, style, or model;
- b. Advertising the goods or services with the intent not to sell them as advertised;
- c. Employing bait-and-switch advertising consisting of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell;
- d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest;
- e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

320. NationsBenefits' unconscionable, false, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Arkansas Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Arkansas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Arkansas Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Arkansas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Arkansas Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Arkansas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

321. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

322. NationsBenefits intended to mislead Plaintiffs and Arkansas Subclass Members and induce them to rely on its misrepresentations and omissions.

323. Had NationsBenefits disclosed to Plaintiffs and Arkansas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NationsBenefits would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. NationsBenefits was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Arkansas Subclass Members. NationsBenefits accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Arkansas Subclass Members acted reasonably in relying on NationsBenefits' misrepresentations and omissions, the truth of which they could not have discovered.

324. NationsBenefits acted intentionally, knowingly, and maliciously to violate Arkansas' Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Arkansas Subclass Members' rights.

325. As a direct and proximate result of NationsBenefits' unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass Members' reliance thereon, Plaintiffs and Arkansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

326. Plaintiffs and the Arkansas Subclass Members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT VIII
CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100 *et seq.*

327. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

328. Plaintiff Ariana Skurauskis (for the purposes of this section, "Plaintiff") brings this claim on behalf of herself and the California Subclass.

329. Plaintiff and California Subclass Members are residents of California.

330. NationsBenefits is a corporation organized or operated for the profit or financial benefit of its owners. NationsBenefits collects consumers' Private Information (for the purposes of

this section, “Private Information”) as defined in the California Consumer Privacy Act (“CCPA”), Cal. Civ. Code § 1798.140.

331. NationsBenefits violated § 1798.150 of the CCPA by failing to prevent Plaintiff’s and California Subclass Members’ nonencrypted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of NationsBenefits’ violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

332. NationsBenefits has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff’s and California Subclass Members’ Private Information. As detailed herein, NationsBenefits failed to do so.

333. As a direct and proximate result of NationsBenefits’ acts, Plaintiff’s and California Subclass Members’ Private Information, including names, contact information, dates of birth, health insurance information, and other sensitive medical records, was subjected to unauthorized access and exfiltration, theft, or disclosure.

334. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure NationsBenefits hereinafter properly safeguards customer Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because NationsBenefits continues to hold customer Private Information, including Plaintiff’s and California Subclass Members’ Private Information. Plaintiff and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected.

335. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by NationsBenefits and third parties with similar inadequate security measures.

336. Plaintiff and the California Subclass seek actual damages, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

337. On June 23, 2023, counsel for Plaintiff Skurauskis provided written notice via certified mail to NationsBenefits at its principal place of business of the intent to pursue claims under the CCPA and an opportunity for NationsBenefits to cure. The domestic return receipt shows that NationsBenefits received the letter. Plaintiff Skurauskis' written notice set forth the violations of NationsBenefits' duty to implement and maintain reasonable security procedures and practices alleged in this Consolidated Complaint.

338. To date, NationsBenefits has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff Skurauskis' counsel.

339. Plaintiff and the California Subclass seek actual damages, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; reasonable attorneys' fees and costs; and statutory damages.

COUNT IX
CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code §§ 1798.80 *et seq.*

340. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

341. Plaintiffs Ariana Skurauskis (for the purposes of this section, "Plaintiff") brings this claim on behalf of herself and the California Subclass.

342. "[T]o ensure that Private Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Private Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect

the Private Information [Private Information] from unauthorized access, destruction, use, modification, or disclosure.”

343. NationsBenefits is a business that owns, maintains, and licenses Private Information (or “Private Information”), within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiff and California Subclass Members.

344. Businesses that own or license computerized data that includes Private Information are required to notify California residents when their Private Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include “the types of Private Information [Private Information] that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

345. NationsBenefits is a business that owns or licenses computerized data that includes “Private Information” [Private Information] as defined by Cal. Civ. Code § 1798.80.

346. Plaintiff’s and California Subclass Members’ Private Information includes “Private Information” as covered by Cal. Civ. Code § 1798.82.

347. Because NationsBenefits reasonably believed that Plaintiff’s and California Subclass Members’ Private Information was acquired by unauthorized persons during the Data Breach, NationsBenefits had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

348. NationsBenefits failed to fully disclose material information about the Data Breach, including the types of Private Information impacted.

349. By failing to disclose the Data Breach in a timely and accurate manner, NationsBenefits violated Cal. Civ. Code § 1798.82.

350. NationsBenefits also violated Cal. Civ. Code § 1798.82 by not publishing a notice of data breach in the format required by Cal. Civ. Code § 1798.82(d)(1).

351. As a direct and proximate result of NationsBenefits' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members suffered damages, as alleged above.

352. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT X
CALIFORNIA UNFAIR COMPETITION ACT
Cal. Bus. & Prof. Code §§ 17200 *et seq.*

353. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

354. Plaintiff Ariana Skurauskis (for the purposes of this section, "Plaintiff") brings this claim on behalf of herself and the California Subclass.

355. NationsBenefits is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

356. NationsBenefits violated Cal. Bus. & Prof. Code §§ 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

357. NationsBenefits' "unfair" acts and practices include:

a. NationsBenefits failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. NationsBenefits failed to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as alleged herein. This conduct, with little if any utility, is unfair when weighed

against the harm to Plaintiff and California Subclass Members, whose Private Information has been compromised;

c. NationsBenefits' failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100;

d. NationsBenefits' failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as alleged above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of NationsBenefits' grossly inadequate security, consumers could not have reasonably avoided the harms that NationsBenefits caused; and

e. NationsBenefits engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

358. NationsBenefits has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, and California common law.

359. NationsBenefits' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and California Subclass Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

h. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

360. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

361. As a direct and proximate result of NationsBenefits' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and suffered monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

362. NationsBenefits acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass Members' rights.

363. Plaintiff and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from NationsBenefits' unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT XI

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. §§ 501.201 *et seq.*

364. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

365. Plaintiffs Anthony Skuya, Renee Fideleff and Stephen Wolsey (for the purposes of this section, “Plaintiffs”) bring this claim on behalf of themselves and the Florida Subclass.

366. Plaintiffs and Florida Subclass Members are “consumers” as defined by Fla. Stat. § 501.203.

367. NationsBenefits advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

368. NationsBenefits engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Florida Subclass Members’ Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Florida Subclass Members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida’s data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs ‘and Florida Subclass Members’ Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Florida Subclass Members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida’s data

security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Florida Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

369. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

370. Had NationsBenefits disclosed to Plaintiffs and Florida Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, NationsBenefits would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. NationsBenefits was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Florida Subclass Members. NationsBenefits accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Florida Subclass Members acted reasonably in relying on NationsBenefits' misrepresentations and omissions, the truth of which they could not have discovered.

371. As a direct and proximate result of NationsBenefits' unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and

identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

372. Plaintiffs and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT XII

ILLINOIS PERSONAL INFORMATION PROTECTION ACT

815 Ill. Comp. Stat. §§ 530/10(a) *et seq.*

373. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

374. Plaintiffs Lenore Caliendo, Kevin McCoy and Sharon McCoy (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the Illinois Subclass.

375. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic Private Information (for the purpose of this section, "Private Information"), NationsBenefits is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

376. NationsBenefits is a Data Collector that owns or licenses computerized data that includes Private Information. NationsBenefits also maintains computerized data that includes Private Information which NationsBenefits does not own.

377. Plaintiffs' and Illinois Subclass Members' Private Information includes "Private Information" as defined by 815 Ill. Comp. Stat. § 530/5.

378. NationsBenefits is required to give immediate notice of a breach of a security system to owners of Private Information which NationsBenefits does not own or license, including Plaintiffs and Illinois Subclass Members, pursuant to 815 Ill. Comp. Stat. § 530/10(b).

379. By failing to give immediate notice to Plaintiffs and Illinois Subclass Members, NationsBenefits violated 815 Ill. Comp. Stat. § 530/10(b).

380. NationsBenefits is required to notify Plaintiffs and Illinois Subclass Members of a breach of its data security system which may have compromised Private Information which NationsBenefits owns or licenses in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

381. By failing to disclose the Data Breach to Plaintiffs and Illinois Subclass Members in the most expedient time possible and without unreasonable delay, NationsBenefits violated 815 Ill. Comp. Stat. § 530/10(a).

382. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

383. As a direct and proximate result of NationsBenefits' violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiffs and Illinois Subclass Members suffered damages, as alleged above.

384. Plaintiffs and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of NationsBenefits' willful violations of 815 Ill. Comp. Stat. § 530/10(a), including equitable relief, costs, and attorneys' fees.

COUNT XIII
ILLINOIS PERSONAL INFORMATION PROTECTION ACT
815 Ill. Comp. Stat. §§ 505 *et seq.*

385. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

386. Plaintiffs Lenore Caliendo, Sadie Brooks, Kevin McCoy and Sharon McCoy (for the purposes of this section, “Plaintiffs”) bring this claim on behalf of themselves and the Illinois Subclass.

387. NationsBenefits is a “person” as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

388. Plaintiffs and Illinois Subclass Members are “consumers” as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

389. NationsBenefits’ conduct as alleged herein was in the conduct of “trade” or “commerce” as defined by 815 Ill. Comp. Stat. § 505/1(f).

390. NationsBenefits’ deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Illinois Subclass Members’ Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Illinois Subclass Members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs’ and Illinois Subclass Members’ Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a) *et seq.*

391. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

392. NationsBenefits intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

393. The above unfair and deceptive practices and acts by NationsBenefits were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

394. NationsBenefits acted intentionally, knowingly, and maliciously to violate Illinois' Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights.

395. As a direct and proximate result of NationsBenefits' unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

396. Plaintiffs and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XIV
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. §§ 510/1 *et seq.*

397. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

398. Plaintiffs Lenore Caliendo, Sadie Brooks, Kevin McCoy and Sharon McCoy (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the Illinois Subclass.

399. NationsBenefits is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

400. NationsBenefits engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

401. NationsBenefits' deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a) *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Illinois Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a) *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a) *et seq.*

402. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

403. The above unfair and deceptive practices and acts by NationsBenefits were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

404. As a direct and proximate result of NationsBenefits' unfair, unlawful, and deceptive trade practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

405. Plaintiffs and Illinois Subclass Members seek all relief allowed by law, including injunctive relief.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT XV

INDIANA DECEPTIVE CONSUMER SALES ACT

Ind. Code §§ 24-5-0.5-1 *et seq.*

406. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

407. Plaintiff Arnisha Marie Shepherd (for the purposes of this section, “Plaintiff”) brings this claim on behalf of herself and the Indiana Subclass.

408. NationsBenefits is a “person” as defined by Ind. Code § 24-5-0.5-2(a)(2).

409. NationsBenefits is a “supplier” as defined by § 24-5-0.5-2(a)(3), because it regularly engages in or solicits “consumer transactions,” within the meaning of § 24-5-0.5-2(a)(1).

410. NationsBenefits engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

411. NationsBenefits’ representations and omissions include both implicit and explicit representations:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff’s and Indiana Subclass Members’ Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff’s and Indiana Subclass Members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Indiana Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Indiana Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Indiana Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Indiana Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

412. NationsBenefits' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

413. The injury to consumers from NationsBenefits' conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Private Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

414. Consumers could not have reasonably avoided injury because NationsBenefits' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the

inadequacy of its data security, NationsBenefits created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

415. NationsBenefits' inadequate data security had no countervailing benefit to consumers or to competition.

416. NationsBenefits' acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. NationsBenefits' failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in NationsBenefits' data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and NationsBenefits concerning the state of NationsBenefits security, and because it is functionally impossible for consumers to obtain credit without their Private Information being in NationsBenefits' systems.

d. Because NationsBenefits took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

417. NationsBenefits also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

418. NationsBenefits intended to mislead Plaintiff and Indiana Subclass Members and induced them to rely on its misrepresentations and omissions.

419. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

420. Had NationsBenefits disclosed to Plaintiff and Indiana Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NationsBenefits would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. NationsBenefits was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and Indiana Subclass Members. NationsBenefits accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Indiana Subclass Members acted reasonably in relying on NationsBenefits' misrepresentations and omissions, the truth of which they could not have discovered.

421. NationsBenefits had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between NationsBenefits and Plaintiff and the Indiana Subclass as alleged herein. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Indiana Subclass—and NationsBenefits, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in NationsBenefits. NationsBenefits' duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

422. NationsBenefits acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff's and Indiana Subclass Members' rights. NationsBenefits' actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

423. NationsBenefits' conduct includes incurable deceptive acts that NationsBenefits engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

424. As a direct and proximate result of NationsBenefits' uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff's and Indiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

425. NationsBenefits' violations present a continuing risk to Plaintiff and Indiana Subclass Members as well as to the general public.

426. Plaintiff and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$500 for each non-willful violation; the greater of treble damages or \$1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT XVI

PROTECTION OF CONSUMER INFORMATION

Kan. Stat. Ann. §§ 50-7a02(a) *et seq.*

427. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

428. Plaintiff A.T. (for the purposes of this section, "Plaintiff") brings this claim on behalf of himself/herself and the Kansas Subclass.

429. NationsBenefits is a person that conducts business in Kansas that owns or licenses computerized data that includes Private Information as defined by Kan. Stat. Ann. § 50-7a02(a).

430. Plaintiff's and Kansas Subclass Members' Private Information (for the purpose of this section, "Private Information") includes "Private Information" as covered under Kan. Stat. Ann. § 50-7a02(a).

431. NationsBenefits is required to accurately notify Plaintiff and Kansas Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass Members' Private Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

432. Because NationsBenefits was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass Members' Private Information, NationsBenefits had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

433. By failing to disclose the Data Breach in a timely and accurate manner, NationsBenefits violated Kan. Stat. Ann. § 50-7a02(a).

434. As a direct and proximate result of NationsBenefits' violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass Members suffered damages, as alleged above.

435. Plaintiff and Kansas Subclass Members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT XVII
KANSAS CONSUMER PROTECTION ACT
K.S.A. §§ 50-623 *et seq.*

436. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

437. Plaintiff A.T. (for the purposes of this section, "Plaintiff") brings this claim on behalf of himself/herself and the Kansas Subclass.

438. K.S.A. §§ 50-623 *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

439. Plaintiff and Kansas Subclass Members are "consumers" as defined by K.S.A. § 50-624(b).

440. The acts and practices alleged herein are “consumer transactions,” as defined by K.S.A. § 50-624(c).

441. NationsBenefits is a “supplier” as defined by K.S.A. § 50-624(l).

442. NationsBenefits advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

443. NationsBenefits engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff’s and Kansas Subclass Members’ Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff’s and Kansas Subclass Members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas’ identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff’s and Kansas Subclass Members’ Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff’s and Kansas Subclass Members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, Kansas’ identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Kansas Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas' identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b; and

h. Omitting, suppressing, and concealing the material fact that it did not implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kansas Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach.

444. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

445. NationsBenefits intended to mislead Plaintiff and Kansas Subclass Members and induce them to rely on its misrepresentations and omissions.

446. Had NationsBenefits disclosed to Plaintiff and Kansas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NationsBenefits would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. NationsBenefits was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and Kansas Subclass Members. NationsBenefits accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Kansas Subclass Members acted reasonably in relying on NationsBenefits' misrepresentations and omissions, the truth of which they could not have discovered.

447. NationsBenefits also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that NationsBenefits knew were substantially one-sided in favor of NationsBenefits (see K.S.A. § 50- 627(b)(5)).

448. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Private Information in NationsBenefits' possession.

449. The above unfair, deceptive, and unconscionable practices and acts by NationsBenefits were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

450. NationsBenefits acted intentionally, knowingly, and maliciously to violate Kansas' Consumer Protection Act, and recklessly disregarded Plaintiff's and Kansas Subclass Members' rights.

451. As a direct and proximate result of NationsBenefits' unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits'

services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

452. Plaintiffs will provide notice of this action to the Attorney General of Kansas.

453. Plaintiff and Kansas Subclass Members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT XVIII
MICHIGAN CONSUMER PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.903 *et seq.*

454. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

455. Plaintiffs Teresa Hassan, Catherine Radtke and Martin Radtke (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the Michigan Subclass.

456. NationsBenefits, Plaintiffs and Michigan Subclass Members are "persons" as defined by Mich. Comp. Laws Ann. § 445.902(d).

457. NationsBenefits advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(g).

458. NationsBenefits engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;
- b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter.

459. NationsBenefits' unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Michigan Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Michigan Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. §§ 445.72 *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Michigan Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Michigan Subclass Members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. §§ 445.72 *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Michigan Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Michigan Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. §§ 445.72 *et seq.*

460. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

461. NationsBenefits intended to mislead Plaintiffs and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

462. NationsBenefits acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Michigan Subclass Members' rights.

463. As a direct and proximate result of NationsBenefits' unfair, unconscionable, and deceptive practices, Plaintiffs and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services;

loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

464. Plaintiffs and Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT XIX

MISSOURI MERCHANDISE PRACTICES ACT

Mo. Rev. Stat. §§ 407.010 *et seq.*

465. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

466. Plaintiff Sara Jean Williams (for the purposes of this section, “Plaintiff”) brings this claim on behalf of herself and the Missouri Subclass.

467. NationsBenefits is a “person” as defined by Mo. Rev. Stat. § 407.010(5).

468. NationsBenefits engaged in “sales” of and “advertisements” for “merchandise” in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(1), (4), (6) and (7).

469. Plaintiff and Missouri Subclass Members purchased or leased goods or services primarily for personal, family, or household purposes.

470. NationsBenefits engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass Members’ Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Missouri Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff and Missouri Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

471. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

472. NationsBenefits intended to mislead Plaintiff and Missouri Subclass Members and induce them to rely on its misrepresentations and omissions.

473. NationsBenefits acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass Members' rights.

474. As a direct and proximate result of NationsBenefits' unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

475. Plaintiff, on behalf of Missouri Subclass Members, seeks all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT XX **NEW JERSEY CONSUMER FRAUD ACT** **N.J. S.A. §§ 56:8-1 *et seq.***

476. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

477. Plaintiff Edward Wilczynski (for the purposes of this section, "Plaintiff") brings this claim on behalf of himself and the New Jersey Subclass.

478. NationsBenefits is a "person," as defined by N.J.S.A. § 56:8-1(d).

479. NationsBenefits sells "merchandise," as defined by N.J.S.A. § 56:8-1(c) & (e).

480. The New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-2 prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise,

misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

481. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. *See Dewey v. Volkswagen AG*, 558 F. Supp. 2d 505, 525 (D.N.J. 2008); *see also Cox v. Sears Roebuck & Co.*, 138 N.J. 2, 19 (1994).

482. “The standard of conduct that the term ‘unconscionable’ implies is lack of ‘good faith, honesty in fact and observance of fair dealing.’” *Cox*, 138 N.J. 2 at 18 (quoting *Kugler v. Romain*, 58 N.J. 522, 544 (1971)). “In addition, ‘[i]ntent is not an essential element’ for allegations related to unconscionable commercial practices to succeed.” *Fennick v. Kay Am. Jeep, Inc.*, 72 N.J. 372, 379 (1977).

483. NationsBenefits’ handling and treatment of Plaintiff” and New Jersey Subclass Members’ Private Information was unconscionable because:

- a. Plaintiff and New Jersey Subclass Members had no choice but to provide their Private Information to NationsBenefits in order to use their NationsBenefits products;
- b. To the extent that written contracts exist between Plaintiff and New Jersey Subclass Members on the one hand and NationsBenefits on the other hand, those written contracts were written by NationsBenefits and were not negotiable;
- c. Once Plaintiff and New Jersey Subclass Members provided their Private Information to NationsBenefits, protection of that Private Information was solely in NationsBenefits’ control. There is no way for Plaintiff and New Jersey Subclass Members to take any reasonable steps on their own to protect the Private Information in NationsBenefits’ hands, nor is there any way that Plaintiff and New Jersey Subclass Members would have any knowledge that it would be necessary for them to take steps on their own to protect their Private Information;

d. NationsBenefits had had prior data security breaches and, thus, knew or should have known that its data security was inadequate and needed to take additional security measures to protect Plaintiff's and New Jersey Subclass Members' Private Information, but failed to do so, even though NationsBenefits was the only entity in a position to protect Plaintiff's and New Jersey Subclass Members Private Information from wrongdoers;

e. Once NationsBenefits became aware of the security breach, it failed to notify Plaintiff and New Jersey Subclass Members of the breach, thus depriving them the opportunity to take measures to protect themselves from the effects of NationsBenefits' failure to protect their Private Information; and

f. NationsBenefits' practices for handing and protecting Plaintiff's and New Jersey Subclass Members' Private Information was contrary to public policy in that NationsBenefits failed to follow FTC guidelines with respect to the protection of Private Information and otherwise failed to follow industry standards for providing reasonable security and privacy measures to protect Plaintiff's and New Jersey Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach.

484. NationsBenefits' handling and treatment of Plaintiff's and New Jersey Subclass Members' Private Information was deceptive because NationsBenefits:

a. Misrepresented that it would protect the privacy and confidentiality of Plaintiff's and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

b. Misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163 *et seq.*;

c. Omitted, suppressed, and concealed the material fact that it did not properly secure Plaintiff's and New Jersey Subclass Members' Private Information; and

d. Omitted, suppressed, and concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163 *et seq.*

485. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

486. NationsBenefits intended to mislead Plaintiff and New Jersey Subclass Members and induce them to rely on its omissions of material fact.

487. NationsBenefits acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's and New Jersey Subclass Members' rights.

488. As a direct and proximate result of NationsBenefits' unconscionable and deceptive practices, Plaintiff and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

489. Plaintiff and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT XXI

NEW YORK GENERAL BUSINESS LAW § 349

N.Y. Gen. Bus. Law § 349

490. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

491. Plaintiffs Michael Wanser and Mary Ann Landries (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the New York Subclass.

492. NationsBenefits engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New York Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and New York Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and New York Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

493. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

494. NationsBenefits acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs and New York Subclass Members' rights.

495. As a direct and proximate result of NationsBenefits' deceptive and unlawful acts and practices, Plaintiffs and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value

of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

496. NationsBenefits' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

497. The above deceptive and unlawful practices and acts by NationsBenefits caused substantial injury to Plaintiffs and New York Subclass Members that they could not reasonably avoid.

498. Plaintiffs and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT XXII

**NORTH CAROLINA IDENTITY THEFT PROTECTION ACT
N.C. Gen. Stat. §§ 75-60 *et seq.***

499. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

500. Plaintiff T.E. (for the purposes of this section, "Plaintiff") brings this claim on behalf of herself and the North Carolina Subclass.

501. NationsBenefits is a business that owns or licenses computerized data that includes Private Information (for the purpose of this count, "Private Information"), as defined by N.C. Gen. Stat. § 75- 61(1).

502. Plaintiff and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

503. NationsBenefits is required to accurately notify Plaintiff and North Carolina Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted

and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

504. Plaintiff's and North Carolina Subclass Members' Private Information includes information as covered under N.C. Gen. Stat. § 75-61(10).

505. Because NationsBenefits discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), NationsBenefits had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

506. By failing to disclose the Data Breach in a timely and accurate manner, NationsBenefits violated N.C. Gen. Stat. § 75-65.

507. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

508. As a direct and proximate result of NationsBenefits' violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass Members suffered damages, as alleged above.

509. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

COUNT XXIII
NORTH CAROLINA UNFAIR TRADE PRACTICES ACT
N.C. Gen. Stat. Ann. §§ 75-1.1. *et seq.*

510. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

511. T.E. (for the purposes of this section, "Plaintiff") brings this claim on behalf of herself and the North Carolina Subclass.

512. NationsBenefits advertised, offered, or sold goods or services in North Carolina and engaged in commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

513. NationsBenefits engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and North Carolina Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and North Carolina Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff's and North Carolina Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

514. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

515. NationsBenefits intended to mislead Plaintiff and North Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

516. Had NationsBenefits disclosed to Plaintiff and North Carolina Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NationsBenefits would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. NationsBenefits was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and North Carolina Subclass Members. NationsBenefits accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and North Carolina Subclass Members acted reasonably in relying on NationsBenefits' misrepresentations and omissions, the truth of which they could not have discovered.

517. NationsBenefits acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass Members' rights.

518. As a direct and proximate result of NationsBenefits' unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged

herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

519. NationsBenefits' conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

520. Plaintiff and North Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT XXIV

**OHIO CONSUMER SALES PRACTICES ACT
Ohio Rev. Code §§ 1345.01 *et seq.***

521. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

522. Plaintiffs Jeffery King, Barbara Kosbab and Lawrence Kosbab (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the Ohio Subclass.

523. Plaintiffs are "persons," as defined by Ohio Rev. Code § 1345.01(B).

524. NationsBenefits was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

525. NationsBenefits advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

526. NationsBenefits engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.02, including:

a. Representing that the subject of a transaction had approval, performance characteristics, uses, and benefits that it did not have;

b. Representing that the subject of a transaction was of a particular standard or quality when they were not.

527. NationsBenefits engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiffs to reasonably protect their interest because of their ignorance of the issues discussed herein;

b. Knowing at the time the consumer transaction was entered into of the inability of the consumer to receive a substantial benefit from the subject of the consumer transaction;

c. Requiring the consumer to enter into a consumer transaction on terms the supplier knew were substantially one-sided in favor of the supplier; and

d. Knowingly making a misleading statement of opinion on which the consumer was likely to rely to the consumer's detriment.

528. NationsBenefits' unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

529. NationsBenefits' representations and omissions were material because they deceived Plaintiffs, and were likely to deceive other reasonable consumers, about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

530. NationsBenefits intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions.

531. NationsBenefits acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiffs' rights.

532. NationsBenefits' unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

533. As a direct and proximate result of NationsBenefits' unfair, deceptive, and unconscionable acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged

herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

534. Pursuant to Ohio Rev. Code § 1345.09(A), each Plaintiff, individually, seeks actual economic damages and non-economic damages of up to five thousand dollars.

535. Pursuant to § Ohio Rev. Code 1345.09(D), Plaintiffs seek declaratory and injunctive relief.

536. Pursuant to Ohio Rev. Code § 1345.09(F), Plaintiffs seek an award of reasonable attorneys' fees.

COUNT XXV
OHIO DECEPTIVE TRADE PRACTICES ACT
Ohio Rev. Code §§ 4165.01 *et seq.*

537. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

538. Plaintiffs Jeffery King, Barbara Kosbab and Lawrence Kosbab (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the Ohio Subclass.

539. NationsBenefits, Plaintiffs, and Ohio Subclass Members are "persons" as defined by Ohio Rev. Code § 4165.01(D).

540. NationsBenefits advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

541. NationsBenefits engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality when they are of another; and

c. Advertising its goods and services with intent not to sell them as advertised.

542. NationsBenefits' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Ohio Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Ohio Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Ohio Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

543. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

544. NationsBenefits intended to mislead Plaintiffs and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

545. NationsBenefits acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Ohio Subclass Members' rights.

546. As a direct and proximate result of NationsBenefits' deceptive trade practices, Plaintiffs and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

547. Plaintiffs and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT XXVI
PENNSYLVANIA UNFAIR TRADE PRACTICES
AND CONSUMER PROTECTION LAW
73 Pa. Cons. Stat. §§ 201-1 *et seq.*

548. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

549. Plaintiff Leroy Fuss (for the purposes of this section, “Plaintiff”) brings this claim on behalf of himself and the Pennsylvania Subclass.

550. NationsBenefits is a “person,” as meant by 73 Pa. Cons. Stat. § 201-2(2).

551. Plaintiff and Pennsylvania Subclass Members purchased goods and services in “trade” and “commerce,” as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

552. NationsBenefits engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

553. NationsBenefits’ unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Pennsylvania Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Pennsylvania Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Pennsylvania Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

554. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

555. NationsBenefits intended to mislead Plaintiff and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

556. Had NationsBenefits disclosed to Plaintiff and Pennsylvania Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NationsBenefits would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. NationsBenefits was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and Pennsylvania Subclass Members. NationsBenefits accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Pennsylvania Subclass Members acted reasonably in relying on NationsBenefits' misrepresentations and omissions, the truth of which they could not have discovered.

557. NationsBenefits acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs and Pennsylvania Subclass Members' rights.

558. As a direct and proximate result of NationsBenefits' unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass Members' reliance on them, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services;

loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

559. Plaintiff and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of \$100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT XXVII

DECEPTIVE TRADE PRACTICES-CONSUMER PROTECTION ACT

Texas Bus. & Com. Code §§ 17.41 *et seq.*

560. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 233 above, as if fully set forth herein.

561. Plaintiffs Kimberly Dekenipp, Wanda Wilson and Dezarae Sanders (for the purposes of this section, "Plaintiffs") bring this claim on behalf of themselves and the Texas Subclass.

562. NationsBenefits is a "person," as defined by the Texas Trade Practices-Consumer Protection Act ("DTPA"), Tex. Bus. & Com. Code § 17.45(3).

563. Plaintiffs and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

564. NationsBenefits advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

565. NationsBenefits engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

566. NationsBenefits' false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Texas Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas' data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Texas Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas' data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Texas Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas' data security statute, Tex. Bus. & Com. Code § 521.052.

567. NationsBenefits intended to mislead Plaintiffs and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

568. NationsBenefits' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NationsBenefits' data security and ability to protect the confidentiality of consumers' Private Information.

569. Had NationsBenefits disclosed to Plaintiffs and Texas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, NationsBenefits would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. NationsBenefits was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Texas Subclass Members. NationsBenefits accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Texas Subclass Members acted reasonably in relying on NationsBenefits' misrepresentations and omissions, the truth of which they could not have discovered.

570. NationsBenefits had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted

professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and Texas Subclass Members, and NationsBenefits because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in NationsBenefits. NationsBenefits' duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiffs and Texas Subclass Members that contradicted these representations.

571. NationsBenefits engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). NationsBenefits engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

572. Consumers, including Plaintiffs and Texas Subclass Members, lacked knowledge about deficiencies in NationsBenefits' data security because this information was known exclusively by NationsBenefits. Consumers also lacked the ability, experience, or capacity to secure the Private Information in NationsBenefits' possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass Members lack expertise in information security matters and do not have access to NationsBenefits' systems in order to evaluate its security controls. NationsBenefits took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiffs' and Texas Subclass Members' Private Information.

573. NationsBenefits intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would

result. The unfairness resulting from NationsBenefits' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from NationsBenefits' unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass Members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

574. NationsBenefits acted intentionally, knowingly, and maliciously to violate Texas' Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiffs and Texas Subclass Members' rights.

575. As a direct and proximate result of NationsBenefits' unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for NationsBenefits' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach. NationsBenefits' unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

576. NationsBenefits' violations present a continuing risk to Plaintiffs and Texas Subclass Members, as well as to the general public.

577. Contemporaneous with the filing of this Consolidated Complaint, pursuant to Tex. Bus. & Com. Code Ann. § 17.501, Plaintiffs' counsel will send to the Consumer Protection Division a copy of the written notice sent to NationsBenefits.

578. On August 17, 2023, counsel for Plaintiffs Kimberly Dekenipp, Wanda Wilson and Dezarae Sanders provided written notice via certified mail to NationsBenefits at its principal place of business of the intent to pursue claims under the DTPA and an opportunity for NationsBenefits to cure. Plaintiffs' written notice set forth the violations of NationsBenefits' duty to implement and maintain reasonable security procedures and practices alleged in this Consolidated Complaint.

579. If, within sixty days after the date of such notification, NationsBenefits fails to provide appropriate relief for their violations of the DTPA, Plaintiffs will amend this Consolidated Complaint to seek damages, including economic damages, damages for mental anguish, statutory damages in the amount of three times the economic and mental anguish damages, as NationsBenefits' acts were committed intentionally or knowingly.

580. Plaintiffs and Texas Subclass Members seek damages, including economic damages, damages for mental anguish, statutory damages in the amount of three times the economic and mental anguish damages, as NationsBenefits' acts were committed intentionally or knowingly, injunctive relief, other equitable relief the Court deems proper, costs, and reasonable and necessary attorneys' fees.

VI. PRAYER FOR RELIEF

WHEREFORE Plaintiffs, individually and on behalf of all others similarly situated, request the following relief:

- A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class Counsel;
- B. A declaration that NationsBenefits breached its duties to Plaintiffs and Class Members;
- C. A mandatory injunction directing NationsBenefits to adequately safeguard the Private Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures;

D. A mandatory injunction requiring that NationsBenefits provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

E. Enjoining NationsBenefits from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

F. An award of damages, including actual, nominal, consequential damages, statutory, and/or punitive, as allowed by law in an amount to be determined;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. For all other Orders, findings, and determinations identified and sought in this Complaint; and

I. Such other and further relief as this court may deem just and proper.

VII. JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for all issues so triable as of right.

Dated: August 23, 2023

Respectfully Submitted,

By: Jeff Ostrow

Jeff Ostrow FBN 121452

KOPELOWITZ OSTROW

FERGUSON WEISELBERG GILBERT

One West Las Olas Blvd., Suite 500

Fort Lauderdale, Florida 33301

Telephone: (954) 332-4200

ostrow@kolawyers.com

*Liaison Counsel for Plaintiffs
and the Putative Classes*

**MORGAN & MORGAN
COMPLEX LITIGATION GROUP**

John Allen Yanchunis FBN 324681
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 275-5272
jyanchunis@forthepeople.com

TYCKO & ZAVAREEI LLP

Sabita J. Soneji (*pro hac vice*)
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
ssoneji@tzlegal.com

BARNOW AND ASSOCIATES, P.C.

Ben Barnow (*pro hac vice*)
205 W. Randolph St., Suite 1630
Chicago, IL 60606
Telephone: (312) 621-2000
b.barnow@barnowlaw.com

*Interim Co-Lead Counsel for Plaintiffs
and the Putative Classes*

**CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.**

James E. Cecchi (*pro hac vice*)
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com

*Federal Coordination and Settlement Liaison
for Plaintiffs and the Putative Classes*